Omni 37xx

Reference Manual

VeriFone Part Number 22412, Revision A

Reference Manual

© 2003 VeriFone, Inc.

All rights reserved. No part of the contents of this document may be reproduced or transmitted in any form without the written permission of VeriFone, Inc.

The information contained in this document is subject to change without notice. Although VeriFone has attempted to ensure the accuracy of the contents of this document, this document may include errors or omissions. The examples and sample programs are for illustration only and may not be suited for your purpose. You should verify the applicability of any example or sample program before placing the software into productive use. This document, including without limitation the examples and software programs, is supplied “As-Is.”

VeriFone, the VeriFone logo, and Omni are registered trademarks of VeriFone. Other brand names or trademarks associated with VeriFone’s products and services are trademarks of VeriFone, Inc.

All other brand names and trademarks appearing in this manual are the property of their respective holders.

Comments? Please e-mail all comments in this document to **Tell_Us_More@VeriFone.com**

VeriFone, Inc.
2455 Augustine Drive
Santa Clara CA 95054-3002

www.verifone.com

VeriFone Part Number 22412, Revision A

CONTENTS

PREFACE 11

Audience 11
Organization 11
Related Documentation 12
Guide Conventions 13

CHAPTER 1
Introduction

Omni 37xx Series of Terminals 15
Features and Benefits 16
Exceptional
Ease Of Use 16
Countertop Performance in a “Hand-Over” Design 16
True Multi-Application Capability 16

CHAPTER 2
Terminal Setup

Select Terminal Location 17
Ease of Use 17
Environmental Factors 17
Electrical Considerations 17
Unpack the Shipping Carton 18
Establish Telephone Line Connections 19
Install Paper Roll 19
Install/Replace MSAM Cards 21
Connect Optional Device(s) 23
Connect PIN Pad, Smart Card Reader, or Bar Code Wand 24
Connect Check Reader 24
External Printers Supported 25
Connect Terminal Power Pack 25

CHAPTER 3
Using the Terminal Keys

Data Entry Modes 28
The Keypad 28
Function Key Descriptions 29
Programmable Function (PF) Key Descriptions 31

CHAPTER 4
System Mode

When to Use System Mode 33
Local and Remote Operations 33
Verifying Terminal Status 34
Entering System Mode 34
File Groups 35
Passwords 35
System Password 35
File Group Passwords 36
System Mode Menus 36
System Mode Procedures 37

Enter and Exit System Mode 38
System Mode Menu 1 39
System Mode Menu 2 40
System Mode Menu 3 43
System Mode Menu 4 49
System Mode Menu 5 51
System Mode Menu 6 52

CHAPTER 5
File Authentication

Introduction to File Authentication 55
The VeriFone Certificate Authority 55
Special Files Used in the File Authentication Process 55
How File Authentication Works 57
Planning for File Authentication 62
Digital Certificates and the File Authentication Process 65
File Authentication and the File System 70
FILESIGN.EXE File Signing Tool 73
FILESIGN.EXE System Requirements 73
Operating Modes for FILESIGN.EXE 74
Command-Line Entries for FILESIGN.EXE 75
Command-Line Mode Syntax Example 75
FILESIGN.EXE Graphical Interface Mode 76

CHAPTER 6
Performing Downloads

Downloads and Uploads 79
Download Methods 79
Download Tools 80
Download Content 80
Full and Partial Downloads 81
Omni 37xx Download Differences 84
Support for Multiple Applications 84
Use of RAM and Flash Memory 85
Redirection of Files During Application Downloads 86
File Authentication Requirements 90
Support for File Compression 98
Effect of Downloads on Existing Files and Data 98
Set Up the Download Environment 99
Cable Connection for Direct Downloads 99
Telephone Line Connection for Telephone Downloads 100
Cable Connection for Back-to-Back Application Downloads 101
Direct Application Downloads 101
Hardware Checklist 101
Software Checklist 101
Checklist for Effects on Files and Settings in the Receiving Terminal 102
Direct Application Download Procedure 102
Direct Operating System Downloads 106
Hardware Checklist 106
Software Checklist 106
Checklist for Effects on Files and Settings in the Receiving Terminal 107
Direct Operating System Download Procedure 107
Download by Telephone 109
Hardware Checklist 109

Software Checklist . . . 109
Telephone Download Procedure . . . 110
Back-to-Back Application Downloads . . . 112
Hardware Checklist . . . 112
Software Checklist . . . 112
Checklist for Effects on Files and Settings in the Receiving Terminal . . . 113
Back-to-Back Application Download Procedure . . . 113

CHAPTER 7 Troubleshooting and Service

Troubleshooting . . . 118
Terminal Display Does Not Show Correct or Readable Information . . . 118
Telephone Line Connection Does Not Work Properly . . . 118
Printer Does Not Work . . . 118
Serial Port Does Not Work . . . 118
Terminal Does Not Process Transactions . . . 118
Keypad Does Not Respond . . . 119
Cleaning and Care . . . 119
VeriFone Service and Support . . . 120
Returning a Terminal . . . 120
Specifications . . . 122
Power . . . 122
DC Power Pack . . . 122
Temperature . . . 122
External Dimensions . . . 122
Weight . . . 122
Accessories and Documentation . . . 123
Power Pack . . . 123
Thermal Printer Paper . . . 123
Paper Roll Spindle . . . 123
VeriFone Cleaning Kit . . . 123
Download Cables . . . 123
Cables for Optional Peripherals . . . 123
Telephone Line Cord . . . 123
Wire Clip . . . 123
Documentation . . . 124

APPENDIX A System Messages . . . 125

APPENDIX B ASCII Table . . . 135

APPENDIX C Port Pinouts . . . 137
PIN Pad Serial Port . . . 137
RS232 Port . . . 137
Telco Port . . . 137
Barrel Connector Polarity . . . 137

GLOSSARY . . . 139

INDEX . . . 147

LIST OF FIGURES

Figure 1	Omni 37xx Product Components	18
Figure 2	Direct Telephone Connection	19
Figure 3	Printer Latch Button	20
Figure 4	Removing Partial Paper Roll	20
Figure 5	Loading Paper Roll	21
Figure 6	Closing Paper Roll Cover	21
Figure 7	MSAM Compartment Door and Optional Locking Screw	22
Figure 8	MSAM Holder Close-Up	22
Figure 9	Using an MSAM Holder	22
Figure 10	Smart Card Reader Connection	24
Figure 11	CR 600 Check Reader Connection	25
Figure 12	Omni 37xx Power Pack Connection	26
Figure 13	Front Panel Key Arrangement	27
Figure 14	The Development Process	59
Figure 15	The Pre-Deployment Process	60
Figure 16	The Deployment Process	62
Figure 17	Certificate Trees in Development and Deployment Terminals	68
Figure 18	Certificate Replacement Process	70
Figure 19	Omni 37xx Application Memory Partitions	71
Figure 20	FileSign Dialog Box for FILESIGN.EXE Under Windows	74
Figure 21	Display Prompts During the File Authentication Process	93
Figure 22	Serial Cable Connection for Direct Downloads	100
Figure 23	Back-To-Back Download Process	115
Figure 24	Information Labels on Bottom of Terminal	121
Figure 25	ASCII Table for the Omni 37xx Display	136

LIST OF TABLES

Table 1	Optional Devices Supported	23
Table 2	Example of Last Character Changing	30
Table 3	Example ALPHA Key Entries	30
Table 4	Using ALPHA and the 12-Key Keypad	30
Table 5	System Mode Menus	36
Table 6	Procedural Description Example	37
Table 7	Enter System Mode	38
Table 8	System Mode Menu 1	39
Table 9	System Mode Menu 2	41
Table 10	System Mode Menu 3	44
Table 11	System Mode Menu 4	49
Table 12	System Mode Menu 5	51
Table 13	System Mode Menu 6	52
Table 14	FILESIGN.EXE tool Filename Extensions	56
Table 15	Executable File Extensions	63
Table 16	Differences Between Required Inputs	69
Table 17	Download File Extensions	73
Table 18	Command-Line Mode Switches for FILESIGN.EXE	75
Table 19	Types of Full and Partial Downloads	82
Table 20	Common Steps to Start a Download	102
Table 21	Direct Application Download Procedure	103
Table 22	Direct Operating System Download Procedure	108
Table 23	Download by Telephone Procedure	110
Table 24	Back-to-Back Application Download Procedure	116

This guide is your primary source of information for setting up and installing the Omni 37xx series of terminals.

Audience

This document has two primary audiences, but is useful for anyone installing and configuring the Omni 37xx terminal:

- **Deployment Administrators** prepare multiple units for deployment to their customers, configuring the units with applications, network configurations, phone numbers, and security. Deployment Administrators may work for a bank, credit card service company, or any company with a vertical application for the Omni 37xx terminal.
- **Local Administrators** integrate and maintain Omni 37xx terminals into a single business site. Business owners or store managers generally perform this function.

Organization

This guide is organized with the following chapters:

Step 1, Introduction. Provides an overview of the Omni 37xx series of units.

Chapter 2, Terminal Setup. Explains set up and installation of the Omni 37xx unit. This chapter tells how to select a location and establish connections with other devices.

Chapter 3, Using the Terminal Keys. Explains the operational features of the Omni 37xx unit and describes how to use the Omni 37xx keys to perform all the data entry or system mode tasks described in this manual.

Chapter 4, System Mode. Describes password-controlled system mode operations, as well as how to use it to perform a variety of test and configuration procedures.

Chapter 5, File Authentication. Describes the file authentication module of the VeriShield security architecture and describes how to use the file signing utility, FILESIGN.EXE, to generate signature files.

Chapter 6, Performing Downloads. Documents procedures for downloading applications and files to Omni 37xx units.

Chapter 7, Troubleshooting and Service. Provides troubleshooting guidelines, should you encounter a problem in terminal installation and configuration. This chapter also discusses cleaning and maintenance, as well as power requirements and dimensions for Omni 37xx terminals. It also provides information on contacting your local VeriFone representative or service provider, and information on how to order accessories or documentation from VeriFone.

This guide also contains appendices for System Messages, Port Pinouts, ASCII Table, and Glossary.

Related Documentation

To learn more about the Omni 37xx terminal, refer to the following set of documents:

- *Omni 37xx Certifications and Regulations*, VeriFone Part Number (VPN) - 22429
- *Omni 3750 Quick Installation Guide*, VPN - 22398
- *Omni 3740 Quick Installation Guide*, VPN - 22407
- *Omni 3720 Quick Installation Guide*, VPN - 22409
- *Omni 3710 Quick Installation Guide*, VPN - 22408
- *Omni 3705 Quick Installation Guide*, VPN - 22403
- *Omni 37xx Series Installation Guide*, VPN - 22399
- *Omni 37xx Privacy Shield Quick Installation Guide*, VPN - 22410
- *Omni 37xx Swivel Stand Quick Installation Guide*, VPN - 22411
- *Omni 37xx Service Guide*, VPN - 22413
- *Verix Programmer's Manual*, VPN - 19733

Guide Conventions

Various conventions are used to help you quickly identify special formatting. The following table describes these conventions and provides examples of their use.

Convention	Meaning	Example
Blue	Text in blue indicates terms that are cross referenced.	See Guide Conventions.
Italics	Italic typeface indicates book titles or emphasis.	You *must* not use this unit underwater.
`ScreenText - PRE`	ScreenText format is used while specifying onscreen text, such as text that you would enter at a command prompt, or to provide an URL.	`http://www.verifone.com`
NOTE	The pencil icon is used to highlight important information.	RS232-type devices do not work with the PIN pad port.
CAUTION	The caution symbol indicates hardware or software failure, or loss of data.	The terminal is not waterproof and is intended for indoor use only.
WARNING	The lighting symbol is used as a warning when bodily injury might occur.	Due to risk of shock do not use the terminal near water.

CHAPTER 1

Introduction

Omni 37xx Series of Terminals

This chapter provides a brief description of the Omni 37xx series of terminals.

The Omni 37xx terminal series represents the shape of things to come in e-payment. The bold ergonomic design is sleek and stylish, offering countertop power and 32-bit performance in an integrated terminal that can be handed to the consumer for input. In addition, the Omni 37xx series serves as the entry point to VeriFone's acclaimed multi-application platform–with the capability to securely support payment and value-added applications on a single terminal.

NOTE

VeriFone ships variants of the Omni 37xx terminal for different markets. Your terminal may have a different configuration. The following devices may or may not be present: a smart card reader, a printer, and/or zero, two, or four SAM holders.

Features At a Glance

- Delivers **power** and **usability** in a **convenient** "hand-over" design.
- Securely supports and runs **payment** and **value-added applications**.
- **Multi-application** operating environment.
- Offers **unsurpassed performance** on **EMV** smart card transactions.
- **32-bit processing** and **multi-tasking** capabilities.
- **Security** architecture meets specifications for PIN-entry devices (PED) and sophisticated **file authentication**.

Features and Benefits

Omni 37xx terminals provide the right combination of features and functions at the right price. This includes a vertical magnetic-stripe card reader, smart card reader, integrated PIN pad, and a quiet, fast, integrated thermal printer (ITP).

Exceptional Ease Of Use

- Bold design is sleek, stylish, and lightweight for conveniently handing terminal to consumer for PIN entry or other input.
- Intuitive ATM-style interface, large 8 line x 21 character backlit display with split screen capabilities, large keys, and extra-size menu prompts simplify training and reduce calls to the Help Desk.
- Integrated high-speed thermal printer simplifies paper loading and virtually eliminates paper jams.
- Triple-track, high-coercivity card reader handles most magnetic stripe cards.

Countertop Performance in a "Hand-Over" Design

- 32-bit processing and multi-tasking capabilities make short work of payment, payment-related, and value-added applications.
- Exceptional graphics-handling capabilities of display and printer quickly render logos, graphical fonts, and character-based languages.
- VeriCentre Appliance Management Suite employs advanced file compression to streamline simultaneous downloads of application software to hundreds of terminals.
- Integrated PIN pad offers added convenience to handle PIN-based applications.
- Ensures uncompromising reliability from VeriFone, the worldwide leader in e-payment.

True Multi-Application Capability

- 1.5 - 6 MB of memory and Verix's dynamic memory allocation support two or three typical-sized applications on a single terminal.
- Primary smart card reader and two to four Security Access Modules (SAMs) safeguard sensitive financial data and support multiple smart card schemes.
- Omni 37xx series of terminals and SoftPay EMV software have received EMV Level 1 and Level 2 Type approval for smart card solutions. The Verix EMV Library provides efficient development of other EMV-compliant applications.
- VeriShield security architecture meets published specifications for PIN-entry devices (PED) and is PED-certified, providing sophisticated file authentication, to prevent execution of unauthorized software on Omni 37xx terminals.

CHAPTER 2

Terminal Setup

This chapter describes the terminal setup procedure. You will learn how to:

- Select a location and protect the terminal from adverse Environmental Factors. See Select Terminal Location.
- Unpack the shipping carton. See Unpack the Shipping Carton.
- Establish telephone line connections. See Establish Telephone Line Connections.
- Install paper roll in the printer. See Install Paper Roll.
- Configure optional peripheral devices. See Connect Optional Device(s).
- Establish power connections. See Connect Terminal Power Pack.

Select Terminal Location

Use the following guidelines described while selecting a location for your Omni 37xx terminal.

Ease of Use

- Select a location convenient for both merchant and cardholder.
- Select a flat support surface, such as a countertop or table.
- Select a location near a power outlet and a telephone/modem line connection. For safety, do not string the power cable in a walkway or place across a walkway on the floor.

Environmental Factors

- Do not use the terminal where there is high heat, dust, humidity, moisture, or caustic chemicals or oils.
- Keep the terminal away from direct sunlight and anything that radiates heat, such as a stove or a motor.
- Do not use the terminal outdoors.

CAUTION

The terminal is not waterproof or dustproof, and is intended for indoor use only. Any damage to the unit from exposure to rain or dust may void any warranty.

Electrical Considerations

- Avoid using this product during electrical storms.
- Avoid locations near electrical appliances or other devices that cause excessive voltage fluctuations or emit electrical noise (for example, air conditioners, electric motors, neon signs, high-frequency or magnetic security devices, or computer equipment).

- Do not use the terminal near water or in moist conditions.

WARNING

Due to risk of shock or terminal damage, do not use the terminal near water, including a bathtub, wash bowl, kitchen sink or laundry tub, in a wet basement, or near a swimming pool.

Unpack the Shipping Carton

Open the shipping carton and carefully inspect its contents for possible tampering or shipping damage. The Omni 37xx is a secure product and any tampering may cause the terminal to cease to function properly.

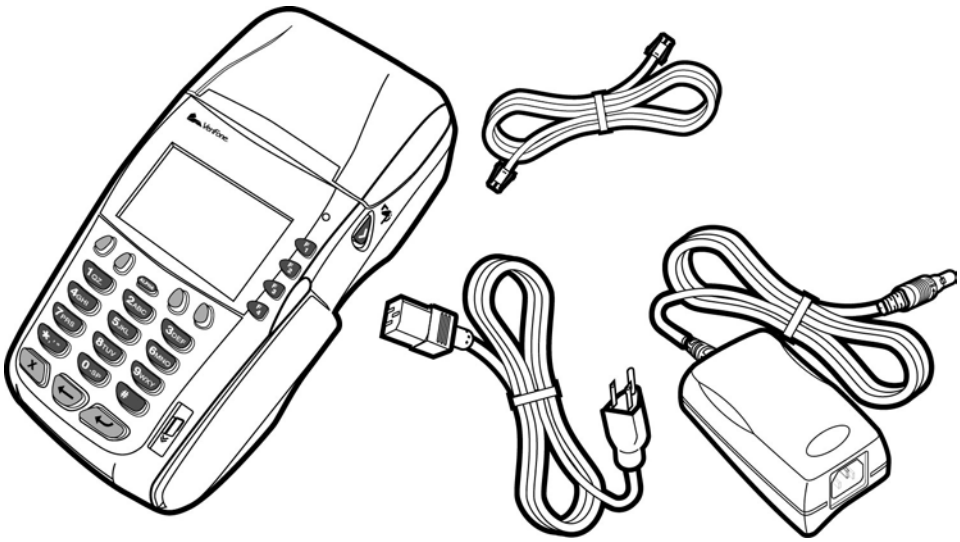


Figure 1 Omni 37xx Product Components

1 Remove and inspect the following items (see Figure 1):

- Omni 37xx terminal
- Power pack
- Telephone line cord

NOTE

VeriFone ships variants of the Omni 37xx terminal for different markets. Your terminal may have a different configuration. The following devices may or may not be present: a smart card reader; a printer; and/or zero, two, or four SAM holders. However, the basic processes described in this guide remain the same, regardless of terminal configuration.

2 Remove all plastic wrapping from the terminal and other components.

3 Remove the clear protective film from the LCD screen.

WARNING

Do not use a terminal that shows signs of damage or tampering.

The Omni 37xx terminal comes equipped with tamper-evident labels. If a label or component appears damaged, please notify the shipping company and your VeriFone representative or service provider immediately.

4 Save the shipping carton and packing material for future repacking or moving the terminal.

Establish Telephone Line Connections

Connect the telephone cord to the communication port on the terminal, then route it directly to a telephone wall jack (see Figure 2). This is a direct connection, and the line is dedicated to the terminal.

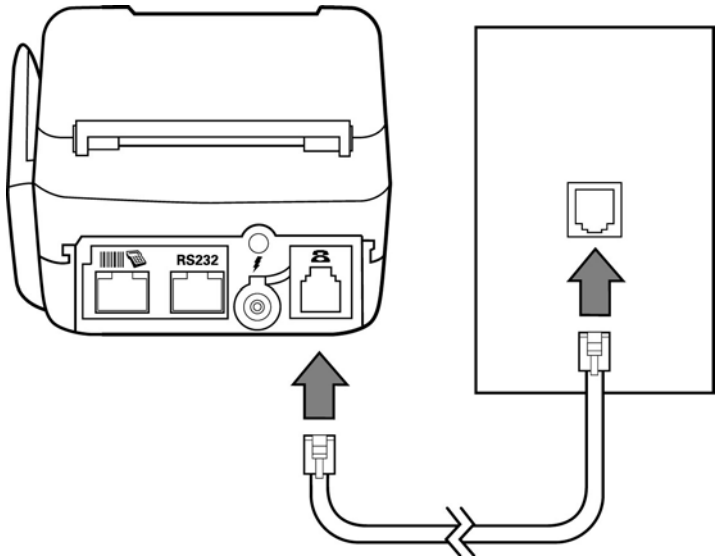


Figure 2 Direct Telephone Connection

CAUTION

To reduce the risk of fire, use only No. 26AWG or larger telecommunication line cord.

Install Paper Roll

A fast, quiet thermal printer is built-in to the Omni 37xx terminal.

Before processing transactions that require a receipt or record, you *must* install a roll of thermal-sensitive paper in the printer.

The internal thermal printer (ITP) uses a roll of single-ply, thermal-sensitive paper 58 millimeters (2.25 inches) wide and approximately 25-33 meters (82-108 feet) long.

WARNING

Poor-quality paper jams the printer. To order high-quality VeriFone paper, refer to Accessories and Documentation.

CAUTION

Store thermal paper in a dry, dark area. Handle thermal paper carefully: impact, friction, temperature, humidity, and oils affect the color and storage characteristics of the paper.

Never load a roll of paper with folds, wrinkles, tears, or holes at the edges or in the print area.

To Install a Paper Roll

1. Turn on the terminal. The green LED indicator will blink on and off, indicating that the printer needs paper.
2. Press the button on the side of the terminal to unlatch the paper roll cover, then rotate the cover up and back (see Figure 3).

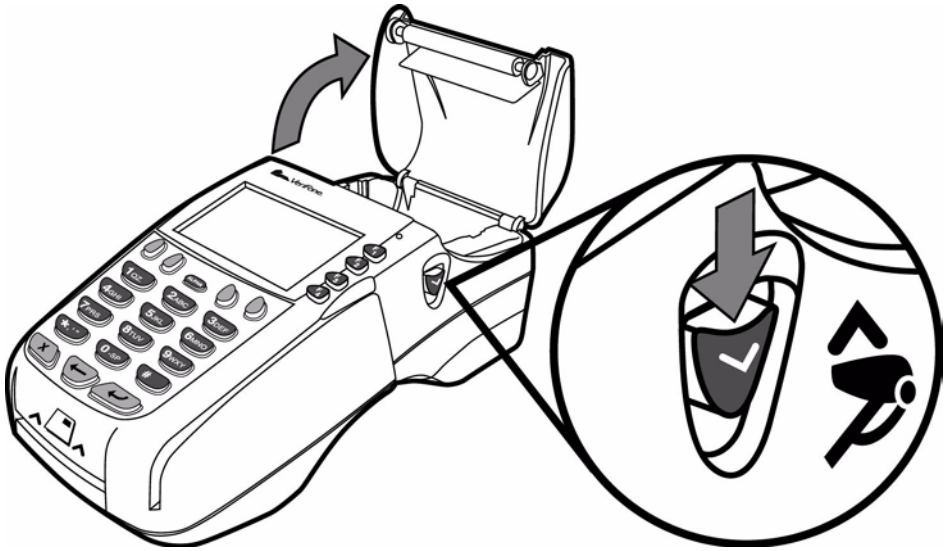


Figure 3 Printer Latch Button

3. Remove partial rolls of paper in the printer tray by lifting up (see Figure 4).

Figure 4 Removing Partial Paper Roll

4. Loosen the glued leading edge of the paper or remove the protective strip from the new roll of paper and cut a straight edge across its leading end.
5. Hold the roll so the paper feeds from the *bottom* of the roll.
6. Drop the paper roll into the printer tray, leaving 7 centimeters (about two inches) of paper sticking up past the serrated metal tear strip (see Figure 5).

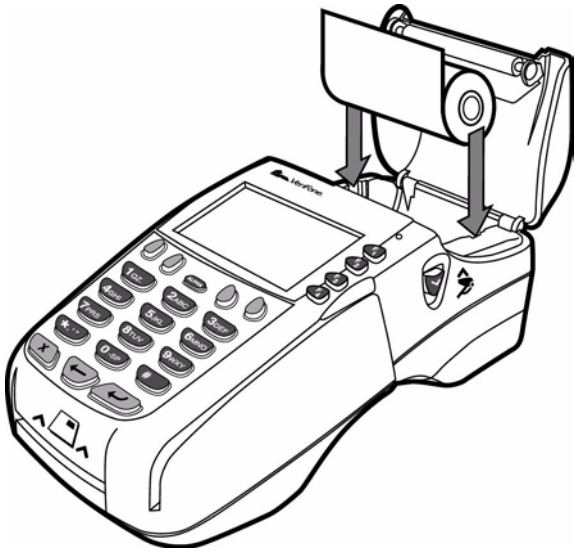


Figure 5 Loading Paper Roll

7 Close the paper roll cover by gently pressing directly on the cover until it clicks shut. Allow a small amount of paper to extend outside the cover (see Figure 6).

NOTE

To prevent damage to the print roller on the paper roll cover, always close the cover by gently pressing down on the paper roll cover.

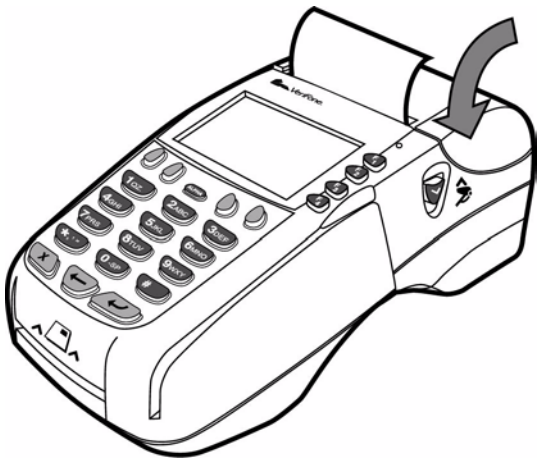


Figure 6 Closing Paper Roll Cover

For paper ordering information, refer to Accessories and Documentation.

Install/Replace MSAM Cards

When you first receive your Omni 37xx terminal, you may need to install one or more MSAM cards, or you may need to replace old cards with new ones.

CAUTION

Observe standard precautions for handling electrostatically sensitive devices. Electrostatic discharges can damage this equipment. VeriFone recommends using a grounded anti-static wrist strap.

To change or install SAMs

1. Remove the power cord from the back of the terminal.
2. Place the terminal upside-down on a soft, clean surface to protect the lens from scratches.
3. To access the MSAM holders, remove the optional locking screw and remove the MSAM compartment door (see Figure 7).

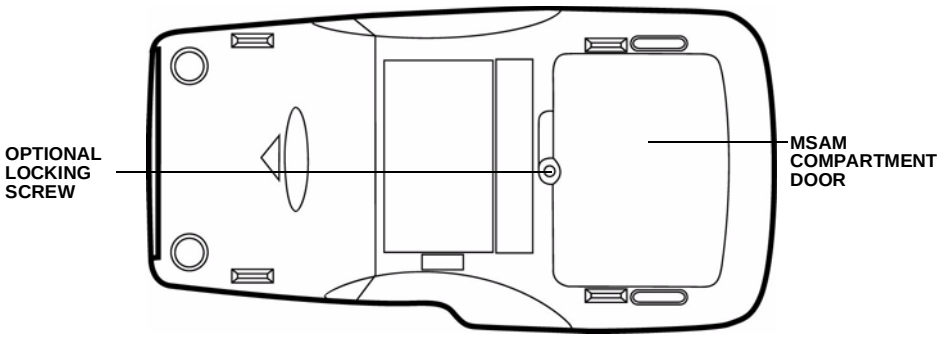


Figure 7 MSAM Compartment Door and Optional Locking Screw

4. Each holder consists of a hinged tilt-up cover attached to a connector base. Unlock a holder by sliding its locking plate to the unlocked position, shown by the OPEN arrow (see Figure 8).

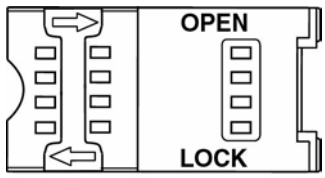


Figure 8 MSAM Holder Close-Up

5. Open the holder by pivoting the cover on its hinges away from its connector base (see Figure 9).

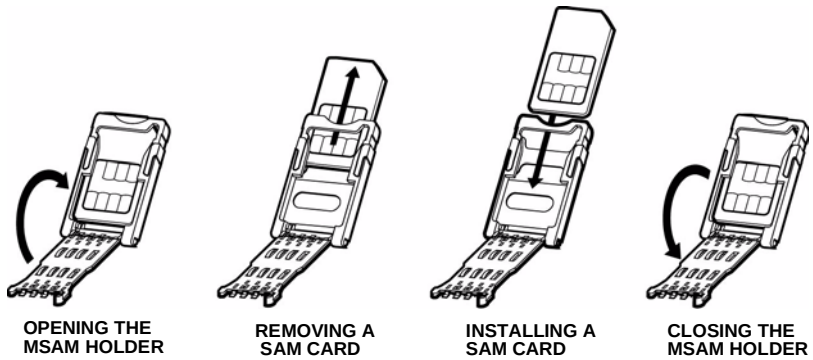


Figure 9 Using an MSAM Holder

6. Remove any previously-installed MSAM card by sliding the card from the cover.

7 Install an MSAM card by aligning the card and carefully sliding it within the guides on the cover until it is fully inserted.

NOTE

Before inserting the MSAM card, position it as shown in Figure 9, with the card's gold contacts facing the smart car reader end of the terminal. The holder connector base has a set of contacts and a notch post on one corner to ensure the MSAM card is positioned correctly when the cover is closed. The MSAM card has a notch on one corner to ensure that it fits into the connector base in only one way.

8 Close the holder by pivoting the cover back to its connector base (see Figure 9).

9 Lock each MSAM holder by sliding its locking plate, as shown by the LOCK arrow, until the plate stops (see Figure 8).

10 Replace the MSAM compartment door and reinstall the optional locking screw (see Figure 7).

Connect Optional Device(s)

The Omni 37xx supports some peripheral devices designed for use with electronic point-of-sale terminals.

Use the two ports on the back panel to connect up to two optional devices.

CAUTION

Before connecting any peripheral device, remove the power cord from the back of the terminal and be sure the LED is not lit. Reconnect the power cord only *after* you are finished connecting the peripheral device(s). For complete information about peripheral installation and use, refer to the user documentation supplied with those devices.

The following sections discuss the most common optional devices supported by this terminal.

Table 1 Optional Devices Supported

Optional Device	Connection Port
Barcode	PIN pad
CR 600	RS232
External LAN	RS232
PIN Pad	PIN pad
RS232 Electronic Cash Register	RS232

Other optional devices may be supported. For more information, please contact your VeriFone distributor.

NOTE

RS232-type devices do not work with the PIN pad port; PIN pad-type devices do not work with the RS232 port. If an optional peripheral device does not function correctly, check the port connection.

Connect PIN Pad, Smart Card Reader, or Bar Code Wand

To Connect PIN Pad, Smart Card Reader, or Bar Code Wand

1. If necessary, insert the small modular plug on one end of the PIN pad cable into the PIN pad's modular jack. For a bar code wand, insert the RJ45-type connector into the PIN pad serial port on the back panel.
2. If installing a PINpad 101, PINpad 201, or PINpad 1000, position and insert the grommet to secure the cable connection.

   If a cable is not already connected to the smart card reader or PINpad 501, insert the small modular plug on one end of the interface cable into the optional device's modular jack.
3. Insert the larger RJ45-type connector on the other end of the PIN pad cable into the PIN pad serial port on the terminal's back panel.

   Figure 10 provides an example of a smart card reader connection to a bar code and PIN pad serial port.

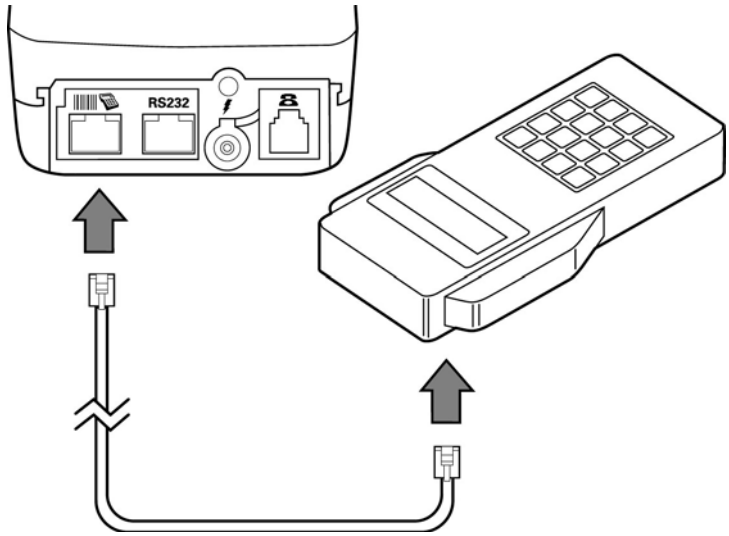


Figure 10 Smart Card Reader Connection

Connect Check Reader

The Omni 37xx terminal supports the CR 600 and CR 1000*i* VeriFone check readers. Contact your VeriFone representative or visit the online store at `www.store.verifone.com` for information on these devices. Figure 11 provides an example of a peripheral connection to an RS232 port.

CAUTION

Check readers require a separate power source. Before connecting a check reader or similar device, remove the power cord from the back of the terminal and be sure the LED is not lit.

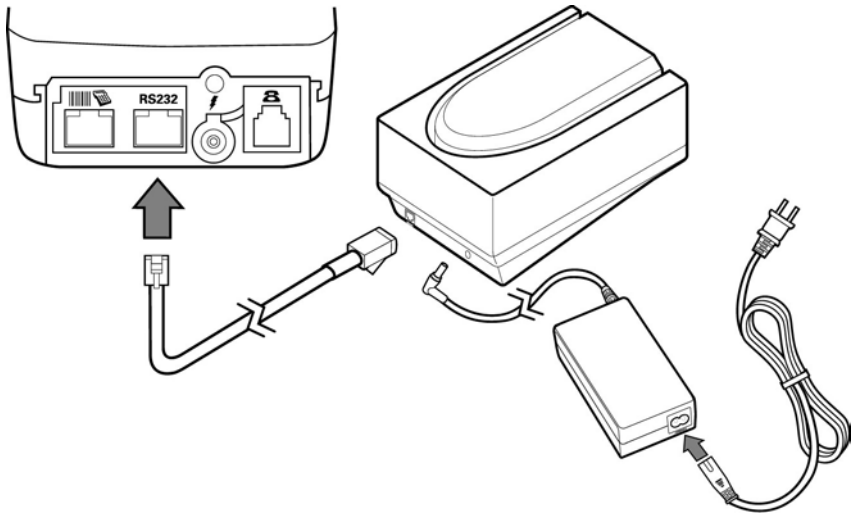


Figure 11 CR 600 Check Reader Connection

External Printers Supported

Although most Omni 37xx variants have an internal thermal printer, it may be convenient to print larger print runs (for example, daily, or weekly reports) to an external printer. The Omni 37xx terminal supports the P250, P350,P900, and P950 VeriFone external printers. Contact your VeriFone representative or visit the online store at `www.store.verifone.com` for information on these devices. External printer connections are through the same port as check readers (see Figure 11).

Connect Terminal Power Pack

When you have finished connecting optional peripheral(s), you are ready to connect the Omni 37xx terminal to a power source.

CAUTION

Using an incorrectly rated power supply may damage the terminal or cause it not to work as specified. Before connecting, ensure that the power supply being used to power the terminal matches the requirements specified at the back of the terminal (see Specifications for detailed power supply specifications). Obtain the appropriately rated power supply before continuing.

WARNING

Do not connect the terminal to the power supply until all the peripherals are attached.

1 Insert the round barrel connector (see Figure 12) into the power port, identified by the icon at right.

NOTE

The round barrel connector on the power pack cable has a plastic lock tab that secures the power cable to the terminal.

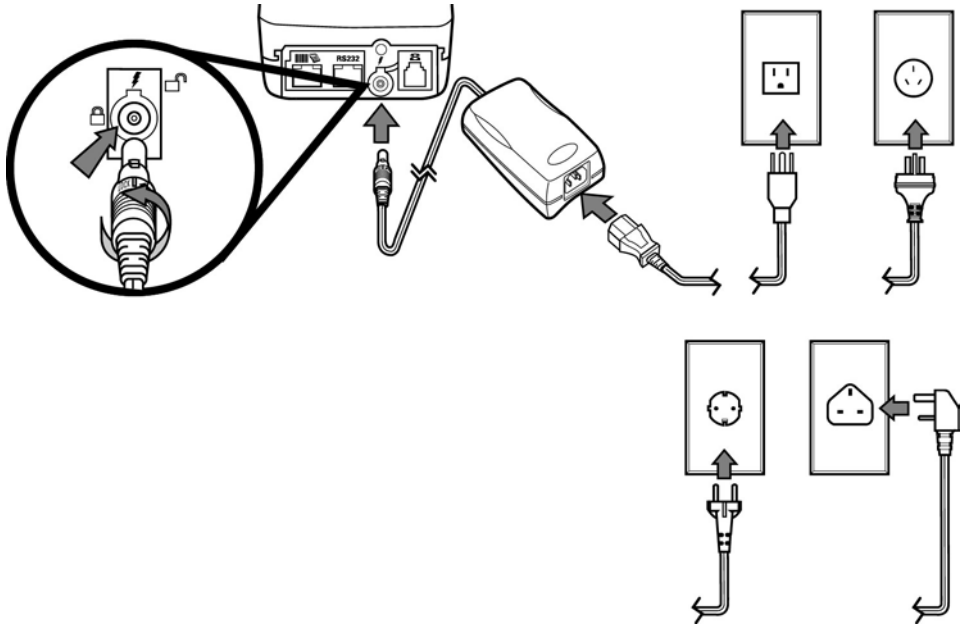


Figure 12 Omni 37xx Power Pack Connection

a To lock the connector into the power port, align the plastic lock tab so it points up. Insert the connector and twist to the left.

b To unlock the connector, twist it to the right.

2 Insert the power cable into the power pack.

3 Plug the power pack cable into a wall outlet or surge protector.

WARNING

Do not plug the power pack into an outdoor outlet or operate the terminal outdoors.

Disconnecting power during a transaction may cause transaction data files not yet stored in terminal memory to be lost.

NOTE

To protect against possible damage caused by lightning strikes and electrical surges, consider installing a power surge protector.

When the terminal has power, the LCD screen lights and the green LED indicator flashes on and off if the printer has no paper, or remains lit if there is paper loaded.

If an application is loaded in the terminal, it starts after the initial VeriFone copyright screen and displays a unique copyright screen. If no application is loaded in the terminal, DOWNLOAD NEEDED appears on screen after the initial VeriFone copyright screen.

Using the Terminal Keys

Before proceeding to other tasks, familiarize yourself with the operational features of the Omni 37xx terminal keypad to enter data.

This section describes how to use the keypad, which consists of a 12-key Telco-style keypad, three color-coded keys below the keypad, the ALPHA key above the keypad, four ATM-style function keys (F1, F2, F3, and F4) to the right of the display (Figure 13), and four *programmable* function (PF) keys directly above the keypad. Using these keys you can perform all data-entry tasks described in this manual. Where a specific key is mentioned, it appears within square brackets (for example, the ALPHA key).

The function keys allow you to navigate though system mode menus and select specific operations.

NOTE

The PF and ATM-style keys can also be assigned application-specific functions in addition to those assigned to system mode operations. These functions are not discussed in this manual.

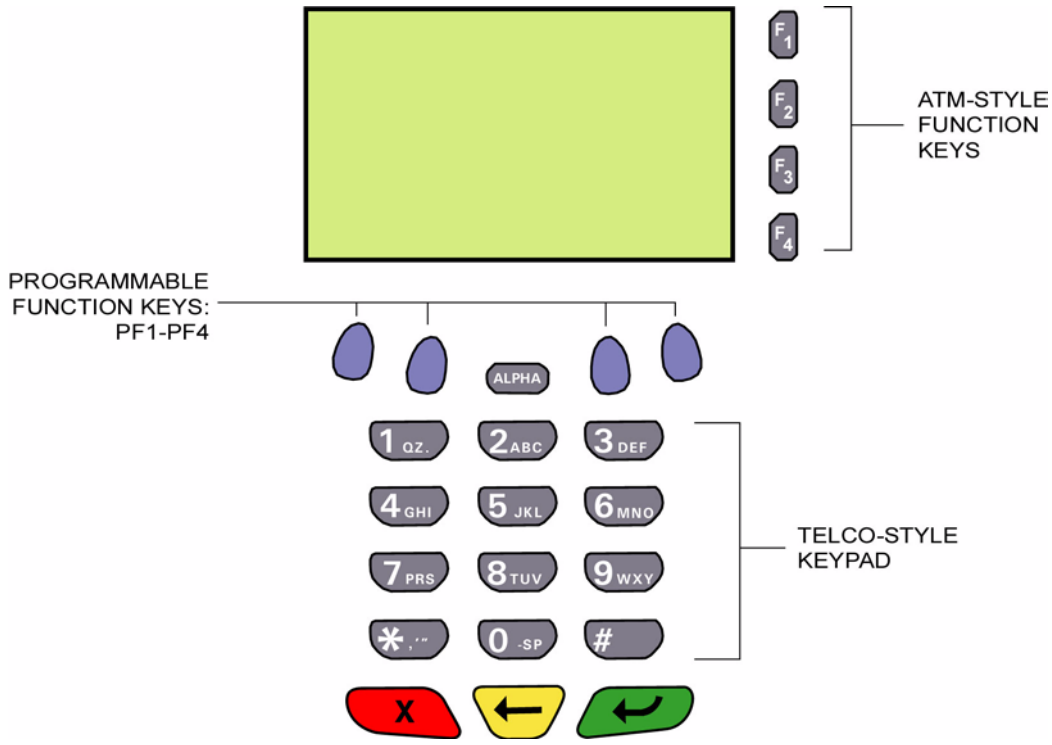


Figure 13 Front Panel Key Arrangement

Data Entry Modes

Before you can use the keys on the front panel to enter ASCII characters, the Omni 37xx must be in a mode that accepts keyed data entry. There are two terminal operating modes, each enables you to press keys to enter data under specific circumstances:

- **Normal mode:** This is the terminal operating mode where an application program is present in memory and currently running.
- **System mode:** This is a special, password-controlled terminal operating mode for performing a variety of test and configuration procedures that cannot be performed when an application is running.

NOTE

If you enter system mode while a terminal application is running in normal mode, system mode preempts the application and takes control of the display and keyboard. The preempted application continues to run in the background, but does not accept user input. The only way to exit system mode is to restart the terminal. For this reason, once you enter system mode, you cannot return to the application in the same session.

If you turn on an Omni 37xx terminal that does not have an application stored in memory, the system prompt `DOWNLOAD NEEDED` appears. You can enter system mode by simultaneously pressing F2 and F4, and then entering the password. Once in system mode, you can configure the terminal as required and perform the necessary download.

If you turn on an Omni 37xx terminal with an application stored in memory, the application executes and the terminal automatically enters normal mode. The application then controls how terminal keys–including the programmable function (PF) keys and the ATM-style keys–process transactions and when you can use specific keys to type characters or respond to prompts.

NOTE

If an application is in terminal memory, the default system password into system mode may have been changed. If so, you must press a special key combination and then type in the required system password to enter system mode. The behavior of key entries depends on the specific active system mode menu.

The Keypad

The keypad is a 13-key arrangement, consisting of a 12-key Telco-style keypad and the ALPHA key (Figure 13).

NOTE

The system mode functions described in the next section require that you enter numbers, letters, or symbols using the keypad.

Using the keypad, you can enter up to 50 ASCII characters, including the letters A–Z, the numerals 0–9, and the following 16 special characters: (*), (,), (‘), (“), (-), (.), (#), (%), (:), (!), (+), (@), (=), (&), (space), and (/).

Function Key Descriptions

The four *programmable* function (PF) keys directly above the keypad allows navigation though the system mode menus and selection of specific terminal operations.

NOTE

The terminal's operating mode and context determine the specific action performed when you press one of the following function keys. The following descriptions are provided solely to acquaint you with some general characteristics of these function keys before presenting more detailed system mode procedure descriptions.

Cancel Key

Pressing the cancel key in normal mode—when the terminal's application is loaded and running—usually has the same effect as pressing the Esc (escape) key on a PC. That is, it terminates the current function or operation.

In system mode, use cancel to perform a variety of functions. The most common use of cancel in system mode is to exit a system mode submenu and return to the main system mode menu. The specific effect of pressing the cancel key depends on the currently active system mode menu.

Backspace Key

In normal mode, the backspace key is commonly used to delete a number, letter, or symbol on the terminal's display screen. Press backspace one time to delete the last character typed on a line. To delete additional characters, moving from right to left, press backspace once for each character or hold down backspace to delete all characters on a line.

In system mode, the specific effect of pressing backspace depends the currently active system mode menu.

ALPHA Key

In normal mode, the ALPHA key enables you to enter one of the two or more characters or symbols assigned to individual keys on the 12-key Telco-style keypad. Use the ALPHA to enter up to 50 different ASCII characters through the following procedure:

1. Press the key on the 12-key keypad that shows the letter or symbol you want (for example, use 2 to type 2, A, B, or C). The number (1–9 or 0) or the symbol (* or #) you pressed now displays.
2. Press ALPHA once to display the first letter. Continuing our example, 2 ALPHA displays the letter A.

3 Continue pressing ALPHA as many times as required to display the desired character. For example, press 2 to display the number 2; press ALPHA once to display the letter A, twice to display B, or three times to display C. If you press ALPHA one more time, you cycle back to the number 2.

NOTE

If you firmly press and hold down one of the keys on the 12-key keypad without using ALPHA, the same character repeats until you stop pressing the key. For example, if you press 2 and hold it down, “2222222...” displays.

If two or more characters display on the Omni 37xx screen, pressing ALPHA changes the last character on the line to the next letter, number, or symbol in the key sequence.

Table 2 Example of Last Character Changing

Keys Depressed	Displayed Characters
Alpha	A5C*A
Alpha	A5C*B
Alpha	A5C*C
Alpha	A5C*D

The following table provides additional examples of how to use the ALPHA key to select ASCII characters from the 12-key Telco-style keypad.

Table 3 Example ALPHA Key Entries

Desired Character	Press Keys
2	2
A	2 ALPHA
S	7 ALPHA ALPHA ALPHA
!	# ALPHA
Space	0 ALPHA ALPHA
Comma (,)	* ALPHA
Plus sign (+)	0 ALPHA ALPHA ALPHA

The following table lists all the ASCII characters you can type using the ALPHA key and the Telco keypad.

Table 4 Using ALPHA and the 12-Key Keypad

Key to Press	Without Pressing ALPHA	Press ALPHA One Time	Press ALPHA Two Times	Press ALPHA Three Times
1 QZ.	1	Q	Z	.
2 ABC	2	A	B	C
3 DEF	3	D	E	F
4 GHI	4	G	H	I
5 JKL	5	J	K	L

Table 4 Using ALPHA and the 12-Key Keypad

Key to Press	Without Pressing ALPHA	Press ALPHA One Time	Press ALPHA Two Times	Press ALPHA Three Times
6 MNO	6	M	N	O
7 PRS	7	P	R	S
8 TUV	8	T	U	V
9 WXY	9	W	X	Y
0 -SP	0	–	[space]	+
* ,' "	*	,	‘	“
#[a]	#	!	:	;

a. The # key also supports additional characters: (@), (=), (&), (/), (\), (%), ($), and (_). To enter @, press # once, then ALPHA four times; to enter =, press # once, then ALPHA five times; to enter &, press # once, then ALPHA six times; etc.

NOTE

In system mode, use ALPHA to key in the default system password, to enter a new system password, and in several other ways (depending on the currently active system mode menu).

Enter Key

In normal mode, the enter key is generally used the same as the enter key on a PC, that is, to end a procedure, confirm a value or entry, answer “Yes” to a query, or select a displayed option.

In system mode, press the enter key to begin a selected procedure, step forwards or backwards in a procedure, and confirm data entries. The specific effect of the enter key depends on the currently active system mode menu.

Programmable Function (PF) Key Descriptions

The row of four PF keys directly above the keypad (Figure 13) from left-to-right are referred to as PF1, PF2, PF3, and PF4. These keys can be assigned application-specific functions. Because such functions are often unique and can vary greatly between applications, they are not discussed in this manual.

The PF keys are also use to toggle through system mode menus. These keys are functioning when arrows appear in the display screen above the associated key, indicating the key’s can be used as follows:

- PF1 ↑ Move to the previous menu or screen
- PF2 ↓ Move to the next menu or screen
- PF3 ← Scroll left
- PF4 → Scroll right

CHAPTER 4

System Mode

This chapter describes a category of terminal functions called *system mode operations*.

- Use a special key combination and password to invoke the system mode. See Entering System Mode.
- Assign files and applications to groups for access control. See File Groups.
- Use system and file group passwords to secure applications and information on the terminal. See Passwords.
- The system mode menus and submenus to configure terminals; download, test, and debug applications; or perform routine tests and terminal maintenance. See System Mode Menus.

System mode is used exclusively by those responsible for configuring, deploying, and managing Omni 37xx terminal installations in the field.

When to Use System Mode

Use system mode functions to perform different subsets of related tasks:

- **Application programmers** configure a development terminal, download development versions of the Omni 37xx application program, then test and debug the application until it is validated and ready to download to other terminals.
- **Deployers of Omni 37xx terminals to end-user sites** perform the specific tasks required to deploy a new Omni 37xx terminal in the field, including configuring the terminal, downloading application software, and testing the terminal prior to deployment.
- **Terminal administrators or site managers** change passwords, perform routine tests and terminal maintenance, and configure terminals for remote diagnostics and downloads by telephone.

To perform the subset of tasks that corresponds to a job, select the appropriate system mode menu(s) and execute the corresponding procedure(s).

Local and Remote Operations

The system mode operations available on an Omni 37xx terminal can be divided into the following two categories or types:

- **Local operations** address a standalone terminal and do not require communication or data transfers between the terminal and another terminal or computer. Perform local system mode operations to configure, test, and display information about the terminal.

- **Remote operations** require communication between the terminal and a host computer (or another terminal) over a telephone line or a cable connection. Perform remote system mode operations to download application software to the terminal, upload software from one terminal to another, and perform diagnostics over a telephone line.

This chapter contains descriptions on how to perform local system mode operations. For information performing remote operations, such as downloads, refer to Chapter 6.

Verifying Terminal Status

The Omni 37xx terminal you are working with may or may not have an application program running on it. After you have set up the terminal (Chapter 2) and the terminal is turned on, use the following guidelines to verify terminal status regarding software and current operating mode:

- If no application program is loaded into terminal RAM or flash, the message `DOWNLOAD NEEDED` appears on the display. From this point, press F2 and F4 to enter system mode and perform the required download.
- If an application program is loaded into terminal RAM or flash, an application-specific application prompt appears. The application is running and the terminal is in normal mode. If all installation steps are complete, the terminal can process transactions.

Entering System Mode

To prevent the unauthorized use of system mode menus, the Omni 37xx terminal firmware requires a system password each time you enter system mode. The default, factory set system password is “Z66831.” Use the following key sequence to enter this password:

1 ALPHA ALPHA 6 6 8 3 1 [↵]

After entering the correct password, the terminal enters system mode and displays the first system mode main menu, `SYS MODE MENU 1`. You can now toggle through all the system mode main menus.

NOTE

It is recommended to enter system mode only on system startup or terminal restart.

If you enter system mode while an application is running, system mode suspends the application and takes control of the display and keyboard. The application idles in the background, but no longer accepts user inputs. You cannot return to the application during that session, only after a restart. In addition, an application running in the background may deny access to certain system mode functions.

File Groups

The Omni 37xx operating system implements a file system in volatile, battery-backed RAM and non-volatile flash memory. Files are assigned to one of 15 groups for access control. Groups are similar to directories on a computer in that different applications can be stored in separate file groups, just like different computer applications can be stored in separate directories. Groups are referred to as *Group n* or *GIDn* throughout this manual.

Each group is protected by a separate password, and each has a separates CONFIG.SYS file. The following rules apply to the Omni 37xx file group system:

- The primary application must be downloaded into Group 1.
- On terminal power up and after a restart, the terminal defaults to Group 1 as the controlling group.
- Group 1 applications have access to files stored in *all* groups. Other applications can reside in Groups 2 through 14.
- Applications in a group other than Group 1 have access only to themselves and files stored in Group 15.
- Group 15 is globally accessible, making it an ideal location for files shared by multiple applications, such as shared libraries.
- File Groups 1 through 15 are empty until they are filled through a download to the Omni 37xx terminal.

For more information on managing file groups, refer to the *Verix Operating System Programmer's Manual* (VPN 19733).

Passwords

CAUTION

If you change a password and then forget it, there is no password recovery method. Without the password, you are unable to access system mode operations and may be prevented from requesting a download, performing remote diagnostics, or changing any of the information already stored in memory. The terminal can, however, continue to process transactions in normal mode.

If you forget or lose the system password to your terminal, please contact your local VeriFone representative for assistance.

System Password

In `SYS MODE MENU 3`, you can select a procedure to change the default password to a unique and more secure password. Once you set a new system password, be sure to secure a copy of the new password.

A valid system password may consist of one to ten alphanumeric characters. You can change the system password at any time, provided you know what the current password is.

When you key in the system password to enter system mode, an asterisk (*) appears on the display for each character you type. These asterisks prevent your password from being seen by an unauthorized person. You can use the ALPHA key to change the characters or symbols you enter; this does not cause additional asterisks to appear.

NOTE

Some application program downloads automatically reset the system password. If your system password no longer works, check if a download has changed your password.

File Group Passwords

From manufacture, each file group uses the default password “Z66831,” entered as:

1 ALPHA ALPHA 6 6 8 3 1, and press [↵]

NOTE

This default password for Group 1 is the same as the password for system mode entry, which is set in the CONFIG.SYS entry *SMPW. The default passwords for Groups 2-15 are blank or empty, and entering the password is accomplished by pressing the enter key. To change passwords, refer to the procedure PASSWORDS F4.

System Mode Menus

The main system mode menus are listed in Table 5.

Table 5 System Mode Menus

SYS MODE MENU 1 CONTRAST F2 CLOCK F3 RESTART F4 ↓	SYS MODE MENU 2 DOWNLOAD F2 RAM FILES F3 FLASH FILES F4 ↑ ↓
SYS MODE MENU 3 CONFIG INFO F2 EDIT F3 PASSWORDS F4 ↑ ↓	SYS MODE MENU 4 REMOTE DIAGS F2 ERROR LOG F3 DEBUGGER F4 ↑ ↓
SYS MODE MENU 5 SCREEN DIAG F2 KEYBOARD DIAG F3 MAG CARD DIAG F4 ↑ ↓	SYS MODE MENU 6 IPP DIAG F2 IPP KEYLOADDIAG F3 PRINTER DIAG F4 ↑ ↓
SYS MODE MENU 7 RAM DIRECTORY F3 FLASH DIRECTORY F4 ↑	

On successful entry of the system password, `SYS MODE MENU 1` appears.

To return to a previous menu, press the PF1 key (below the up arrow). To go to the next menu, press the PF2 key (below the down arrow). To return to the main system mode menu and cancel any changes, press the cancel key.

Each menu has items to select; sometimes these items contain submenus or a series of prompts. When prompted to enter alphabetic or special characters, use the procedure described in Chapter 3.

When performing downloads or operations that change or clear files, the password for each file group is required. The password is only required once per session per file group.

System Mode Procedures

The procedures in this section explain how to use each of the system mode menus listed in Table 5. Each procedure description starts at a main system mode menu. Each procedure takes you step-by-step through a complete system mode operation in the following sequence:

1. When a main system mode menu appears, select an operation by pressing the appropriate key.
2. Complete the operation.
3. Return to the main system mode menu.

NOTE

Before entering system mode and selecting the function(s) to perform, please verify that you have completely installed the Omni 37xx as described in Chapter 2, that the terminal is connected to a power source, and that the terminal is turned on.

Procedure descriptions are arranged in the following tabular format:

Table 6 Procedural Description Example

Display	Action
SUBMENU	

The *Display* column indicates what appears on the terminal display at each step of the procedure. Please note the following conventions used in this column:

- If a prompt or message appears on the screen exactly as it is described, it is shown in Arial font and in ALL CAPS. For example, DOWNLOAD NEEDED.
- If text is enclosed in parentheses, the actual text or message may vary depending on the terminal version you have. For example, (Application Prompt), in which the normal font is used, and text is typed in initial caps.

The *Action* column provides a procedure description that:

- Describes the current step and context of the procedure.
- Indicates the entries to perform using the keypad in response to a prompt or message.

- Provides additional explanations or information about the steps of that particular system mode menu.

A *Submenu* row indicates a specific procedure evoked from a main menu screen. A description of that procedure immediately follows the Submenu row. The following keys have the same function from all submenus:

- Press the enter key to save changes from a submenu and return to the menu screen.

- Press the cancel key to exit any submenu without saving changes.

Enter and Exit System Mode

To enter system mode after you have turned on the Omni 37xx terminal, follow the procedure described in Table 7.

NOTE

On successful completion, some operations automatically exit system mode and restart the terminal. Other operations require that you exit system mode and restart the terminal. To manually exit system mode, select `RESTART F4` in `SYS MODE MENU 1`.

Table 7 Enter System Mode

Display	Action
VERIFONE OMNI Q50015A2 8/12/2003 Verix COPYRIGHT 1997-2003 VERIFONE ALL RIGHTS RESERVED	At startup, the terminal displays a copyright notice screen that shows the terminal model number, the version of the Omni 37xx system firmware stored in the terminal's flash memory, the date the firmware was loaded into the terminal, and the copyright notice. This screen appears for three seconds, during which time you can enter system mode by simultaneously pressing F2 and F4. You can extend the display period of this screen by pressing any key during the initial three seconds. Each key press extends the display period an additional three seconds.
(Application Prompt) or DOWNLOAD NEEDED	If an application already resides on the terminal, an application-specific prompt displays. If no application resides on the terminal, the following message displays: DOWNLOAD NEEDED To enter system mode from this screen, simultaneously press F2 and F4.

Table 7 Enter System Mode

Display	Action
SYSTEM MODE ENTRY PASSWORD ----------	If an application prompt appeared in Step 2 and you chose to enter system mode you are prompted to type the system password. If DOWNLOAD NEEDED appeared in Step 2, use the default password "Z66831." This password is entered as: 1 ALPHA ALPHA 6 6 8 3 1, and press [↵] Use the backspace [←] key to delete the entry and correct any mistakes. If you enter an incorrect password, the terminal exits the SYSTEM MODE ENTRY screen. Verify your password and re-enter it. To quit this operation and return to the application prompt or DOWNLOAD NEEDED screen, press the cancel key.
SYS MODE MENU 1 CONTRAST F2 CLOCK F3 RESTART F4 ↓	SYS MODE MENU 1 is the first menu to display. To toggle through to the other main menus, press the PF2 key or [↵] until you reach the desired menu.

System Mode Menu 1

In this menu you can adjust the display contrast, set the terminal clock, and exit system mode.

Table 8 System Mode Menu 1

Display	Action
SYS MODE MENU 1 CONTRAST F2 CLOCK F3 RESTART F4 ↓	To adjust the display contrast, select CONTRAST F2. To set the date and time, select CLOCK F3. To restart the terminal, select RESTART F4. To toggle to system mode menu 2, press PF2 or [↵].
CONTRAST F2	
SYS MODE CONTRAST CONTRAST UP F2 CONTRAST DOWN F3 ↑	Select CONTRAST UP F2 to increase display contrast or CONTRAST DOWN F3 to decrease display contrast. To return to the main menu and save your changes, press [↵].

Table 8 System Mode Menu 1

Display	Action
CLOCK F3	
Note: The terminal clock is battery-backed to retain date and time settings when the terminal is shut off.	
SYS MODE CLOCK YEAR: 2003 MONTH: 02 DAY: 07 ↑ ↓	This example shows February 07, 2001. To set YEAR, press F2 and type a four-digit number for the current year. To set MONTH, press F3 and type a two-digit number for the current month (between 01–12). To set DAY, press F4 and type a two-digit number for the current day (between 01–31). To save your changes and return to SYS MODE MENU 1, press the PF1 key. To set the time, go to the next submenu. **Note:** The terminal only accepts entries in the format and range specified above. Errors are not highlighted; *you must ensure each entry is correct*. To correct a mistake, press the field's function key (for example, F2 for YEAR) and type a new entry.
SYS MODE CLOCK HOUR: 17 MINUTE: 32 ↑	This example shows 5:32 P.M. To set HOUR, press F2 and type a two-digit number between 00–23 (using the twenty-four hour clock). To set MINUTE, press F3 and type a two-digit number between 01–59. **Note:** The terminal only accepts entries in the format and range specified above. Errors are not highlighted; therefore, you *must* ensure each entry is correct. To correct a mistake, press the field's function key (for example, F2 for HOUR) and type a new entry. To return to the previous menu to set the date, press the PF1 key. To save your changes and return to SYS MODE MENU 1, press enter.
RESTART F4	
RESTART	Select RESTART F4 to exit system mode and restart the terminal.

System Mode Menu 2

In this menu, you can accomplish full or partial downloads to your terminal, clear RAM files, and clear flash files.

NOTE

Before performing a download to flash memory in an initialized terminal (one that contains an application), reclaim all available flash space. Unlike RAM, unused flash and duplicate flash information are not automatically reclaimed during a download. To reclaim this space perform a defrag operation from system mode (refer to the procedure FLASH FILES F4). This operation makes all files in flash contiguous. You must also clear some or all flash memory if your terminal does not have enough space for the impending download.

You cannot perform download, clear, and defragment operations if you entered system mode while an application is running. If you see the message `APPLICATION ALREADY RUNNING, PLEASE RESTART`, press the cancel key and restart the terminal from system mode menu 1. When you see the copyright notice screen, enter system mode within 3 seconds (before the application begins).

Table 9 System Mode Menu 2

Display	Action

`SYS MODE MENU 2`
`DOWNLOAD F2`
`RAM FILES F3`
`FLASH FILES F4`
↑ ↓
	To download an application to your terminal, select `DOWNLOAD F2`. To clear RAM files, select `RAM FILES F3`. To clear flash files, select `FLASH FILES F4`.
	To return to the previous system mode menu, press the PF1 key.
	To return immediately to `SYS MODE MENU 1`, or to quit any operation within this menu, press the cancel key.
	To toggle to `SYS MODE MENU 3`, press the PF2 key or [↵].

DOWNLOAD F2	
`SYS MODE FILE` `FILE GROUP _1`	Type the number of the file group (1 for the primary application; between 1–15 for other applications) to perform the download. (Refer to Chapter 6 for detailed download instructions and information.) After you type a file group number, press [↵].

`SYSTEM MODE FILE`
`GROUP nn PASSWORD`
`----------`
	To continue, enter the required password. If you enter an incorrect password, the following message appears:
	`SYS MODE PASSWORD`
	`PLEASE TRY AGAIN`
	Press [↵]. Verify your password and re-enter it.

`SYS MODE DOWNLOAD G _1`
`FULL F3`
`PARTIAL F4`
↑
	For a full download, select `FULL F3`. For a partial download, select `PARTIAL F4`. (Refer to Chapter 6 for detailed download instructions and information.)
	To return to the main menu, press the PF1 key.

Table 9 System Mode Menu 2

Display	Action
SYS MODE DOWNLOAD G _1 MODEM F2 COM1 F3 COM2 F4 ↑	Select a download mode: MODEM F2, COM1 F3, or COM2 F4. To return to the main menu without saving your selection, press the cancel key.
SYS MODE DOWNLOAD G _1 ***------- DOWNLOADING NOW	The terminal is ready to receive a download. During the download, a line of asterisks appears that shows percentage of completion. Each asterisk equals approximately 10% of the download. You can cancel a download by pressing the cancel key during the download; doing so restarts your terminal.
RAM FILES F3	
SYS MODE RAM CLEAR GROUP _1 F2 CLEAR ALL FILES F3	To clear a file group's RAM files, type the file group number (1–15) and press F2. To correct a mistake, press [←] to delete the number, and type a new entry. CONFIG.SYS protected records that begin with * or # are retained when you clear a RAM file group. To clear the RAM of all file groups, select CLEAR ALL FILES F3. This operation also clears the CONFIG.SYS files from all groups except Group 1. Records that begin with * or # in Group 1 are retained. **Note:** If you have not previously entered a group's password in this session, the terminal prompts for the group's password prior to clearing that group's RAM files.
SYSTEM MODE FILE GROUP nn PASSWORD ----------	To continue, enter the required password. If you enter an incorrect password, the following message appears: SYS MODE PASSWORD PLEASE TRY AGAIN Press [↵]. Verify your password and re-enter it.
SYS MODE CONFIRM G 1 CANCEL F3 CONFIRM F4	To cancel the operation, select CANCEL F3. To continue the operation, select CONFIRM F4. After the operation is complete, you return to the main menu.

Table 9 System Mode Menu 2

Display	Action
FLASH FILES F4	
SYS MODE FLASH CLEAR GROUP _1 F2 CLEAR ALL FILES F3 DEFRAG 0 F4	To clear a file group's flash files, type the file group number (1–15) and press F2. To correct a mistake, press [←] to delete the number, and type a new entry. To clear the flash files of all file groups, press F3. If you have not previously entered a group's password in this session, the terminal prompts you for the group's password prior to clearing that group's flash files. **Caution:** Clearing all flash files erases the application program from your terminal. A new application download is then required. To defragment flash files, press F4, then skip to SYS MODE CONFIRM of this procedure. The number displayed beside DEFRAG is the total amount of space, in bytes, to reclaim in the defrag operation.
SYSTEM MODE FILE GROUP nn PASSWORD ----------	To continue, enter the required password. If you enter an incorrect password, the following message appears: SYS MODE PASSWORD PLEASE TRY AGAIN Press [↵]. Verify your password and re-enter it.
SYS MODE CONFIRM G 1 CANCEL F3 CONFIRM F4	To cancel the operation, select CANCEL F3. To continue the operation, select CONFIRM F4. After the operation is completed, you are returned to the main SYS MODE MENU 2 screen. If you selected DEFRAG in SYS MODE FLASH and select CONFIRM F4 here, you are taken to SYS MODE DEFRAG.
SYS MODE CLEAR CLEARING FLASH PLEASE WAIT	This operation may take a few seconds. If you have cleared all flash files, the terminal displays DOWNLOAD NEEDED on restart. If after clearing selected flash files you experience difficulties with your application, you may have accidentally deleted a flash file that the CONFIG.SYS file in File Group 1 uses. This type of error usually generates the error message RUN FAILED when trying to execute the application; you must restore the required File Group 1 flash file.
SYS MODE DEFRAG RECLAIMING FLASH PLEASE WAIT	This message indicates the flash files are being defragmented; this operation may take a few seconds. On successful completion, the terminal automatically restarts.

System Mode Menu 3

In this menu, you can view terminal configuration information, edit the CONFIG.SYS or another keyed file, and change system mode and file group passwords.

NOTE

Some application program downloads automatically reset the system password.

Table 10 System Mode Menu 3

Display	Action

`SYS MODE MENU 3`
`CONFIG INFO F2`
`EDIT F3`
`PASSWORDS F4`
↑ ↓
	To view terminal configuration information, select `CONFIG INFO F2`. To edit the CONFIG.SYS or another keyed file, or to set the country code for your terminal's modem, select `EDIT F3`. (For more information, refer to the Edit Keyed Files section that follows this main menu description.)
	To change the system mode and file group passwords, select `PASSWORDS F4`. Group 1 and system mode all use a default password that is pre-set at the factory: Z66831. It is entered as: 1 ALPHA ALPHA 6 6 8 3 1 and press [↵]. The default passwords for Groups 2-15 are blank or empty, and entering the password is accomplished by pressing the enter key. To change passwords, refer to the procedure PASSWORDS F4.
	To return to the previous system mode menu, press the PF1 key.
	To return immediately to `SYS MODE MENU 1`, or to quit any operation within this menu, press the cancel key.
	To toggle to the system mode menu 4, press the PF2 key or [↵].

CONFIG INFO F2	

`SYS MODE CONF`
`RAM FILES 22`
`INUSE 48834`
`AVAIL 390010`
`FLASH FILES 1`
`INUSE 5680`
`AVAIL 715208`
↓
	This screen shows the number of kilobytes in use and that available for RAM and flash.
	To continue, press the PF2 key.

Table 10 System Mode Menu 3

Display	Action
SYS MODE CONF RAM 512 FLASH 1024 SERNO xxxxxxxxx PTID 12000000 PART xxxxxxxxx VERS A ↑ ↓	This screen shows configuration information specific to your terminal: • Total kilobytes of RAM memory • Total kilobytes of flash memory • Serial number • Permanent terminal identification number (PTID) • Terminal part number • Terminal hardware version number Your terminal's screen may vary depending on your terminal's model and the operating system version installed. To return to the previous menu, press the PF1 key; to continue, press the PF2 key.
SYS MODE CONF MODL OMNI3700 CTRY US KEYPAD 0 DISPLAY 128064 MAG RDR 0 PRINTER 1 ↑ ↓	This screen shows additional configuration information specific to your terminal: • Model number • Country of manufacture • Keypad type (0 = Telco, 1 = calculator, 2 = Singapore) • Display unit type • Magnetic stripe card reader type • Whether or not a thermal printer is integrated into the terminal (where 0 = No, 1 = Yes) To return to the previous menu, select the PF1 key; to continue, select the PF2 key. To return to the main menu, press the cancel key.
SYS MODE CONF PINPAD 1 LIFE 26778 RSET 971117023334 RCNT 90 MODEM 22 MODEM TYPE 2 ↑	This screen shows additional configuration information specific to your terminal: • Whether or not a PIN pad device is integrated into the terminal (where 0 = No, 1 = Yes) • Number of seconds the terminal has run (LIFE) • Last reset date and time, in YYMMDDHHMMSS format (where YY = year, MM = month, DD = day, HH = hour, MM = minute, and SS = second) • Number of times the terminal has been reset (RCNT) • Modem country code • Modem type (2400bps, 14.4kbps, ISDN, etc.) To return to the previous menu, select the PF1 key; to return to the main menu, press the cancel key.

Table 10 System Mode Menu 3

Display	Action
EDIT F3	
SYS MODE FILE FILE GROUP _1	To search for keyed records in a particular file group, type the appropriate group number and press [↵]. If you cannot locate a particular keyed record, it may be stored in another file group. To search for keyed records in another file group, return to the main menu by pressing the cancel key, then type the appropriate group number and press [↵]. To correct a mistake, press [←] to delete the number and type the new entry.
SYSTEM MODE FILE GROUP nn PASSWORD ----------	To continue, enter the required password. If you enter an incorrect password, the following message appears: SYS MODE PASSWORD PLEASE TRY AGAIN Press [↵]. Verify your password and re-enter it.
SYS MODE EDIT G 1 FILE CONFIG.SYS_ -----------	To edit the CONFIG.SYS file, press [↵]. **Note:** In this menu, you can create a new keyed file or edit an existing one. First, use [←] to clear any previous key name from the display. Then, type the key name, press [↵] and skip to the SYS MODE EDIT VALUE screen below.
SYS MODE EDIT G 1 KEY (Key name)-------- ------------------	To create or search for a keyed record, use [←] to clear any previous key name from the display. Then, type the key name, press [↵], and skip to Step 5b of this procedure. To scroll through the search keys, press [↵], or use the PF1 or PF2 keys to scroll the up and down respectively, as needed. To scroll through keyed records, press either the PF3 or the PF4 key, below the Left and Right arrows respectively, as needed.

Table 10 System Mode Menu 3

Display	Action
SYS MODE EDIT G 1 (Key name) KEY F2 (Key value) VALUE F3 ↑ ↓ ← →	To scroll through the search keys, press [↵]. Or use the PF1 or PF2 keys to scroll the up and down respectively, as needed. To manually enter another key name, select KEY F2 and use [←] to clear the previous key name from the display. Then, type the appropriate key name and press [↵]. To scroll through the displayed key value, press either the PF3 or the PF4 key, below the Left and Right arrows respectively, as needed. To edit a key value, select VALUE F3 and proceed to the next step.
SYS MODE EDIT G 1 KEY (Value)-------- ----------	To create or edit a key value, use [←] to clear any previous key value from the display. Then, type the new key value and press [↵].
SYS MODE EDIT G 1 (Key name) KEY F2 (Key value) VALUE F3 ↑ ↓ ← →	To exit SYS MODE EDIT after completing your edit operations, press the cancel key twice.
PASSWORDS F4	
SYS MODE PASSWORD FILE GROUP _1 F2 SYS MODE ENTRY F3	To change the password of File Group 1, select FILE GROUP _1 F2. Then, go to SYSTEM MODE FILE GROUP nn PASSWORD below. To change the password of another file group, type the appropriate file group number and press F2. Then, go to SYSTEM MODE FILE GROUP nn PASSWORD below. To correct a mistake, press [←] to delete the number, and type the new entry. To change the system password, select SYS MODE ENTRY F3. Then, skip to SYS MODE PASSWORD NEW below. **Note:** Some application program downloads automatically reset the system mode password.

Table 10 System Mode Menu 3

Display	Action
SYSTEM MODE FILE GROUP nn PASSWORD ----------	Type the current password for the selected file group and press [↵]. If you enter an incorrect password, the following message appears: SYS MODE PASSWORD PLEASE TRY AGAIN Press [↵]. Verify your password and re-enter it.
SYS MODE PASSWORD G _1 NEW ----------	Type the new password and press [↵]. To correct a mistake, press [←] to delete the number, and then type the new entry.
SYS MODE PASSWORD G _1 AGAIN ----------	The terminal requests that you verify the new password. Retype the new password and press [↵].
SYS MODE PASSWORD G _1 PASSWORD CHANGED	The new password is now in effect. To exit this screen, press [↵]. You are returned to the main menu.

NOTE

When entering any password, an asterisk (*) appears on the display for each character you type. These asterisks prevent your password from being seen by an unauthorized person. Pressing the ALPHA key changes the characters or symbols you enter, but ALPHA does not cause additional asterisks to appear. Secure a copy of every password to ensure it is not forgotten or lost.

Edit Keyed Files

A *keyed* file is a collection of individual records, which contain ASCII data and are identified by unique search keys. You can edit the ASCII data directly from the terminal keypad using the terminal's built-in keyed file editor. Each record has two parts: a key name and a key value. The search key is a variable-length string, or *key name*, that identifies the record. The information assigned to the search key is contained in a separate variable-length string, or *key value*.

For example, in CONFIG.SYS, the VeriCentre key for the application serial ID number is *ZT. The value for the key is the actual application ID number. By entering *ZT using the editor, the terminal can quickly locate the application serial ID number. You can also use [↵] to scroll through the search keys instead of entering the characters *ZT through the keypad.

NOTE

For a complete list of the ASCII characters supported by the Omni 37xx, as well as their decimal and hexadecimal equivalents, please refer to Appendix B.

CONFIG.SYS: Protected and Non-protected Records

The concept of protected and non-protected records applies only to the CONFIG.SYS files in your terminal. Protected records are those with search keys beginning with an asterisk (*) or a pound symbol (#).

Prior to a download, the recommended procedure is to clear RAM files. Protected records in the File Group 1 CONFIG.SYS file are retained in a full application download and when RAM is cleared. Non-protected records are all other CONFIG.SYS files, and records of other files. These records are deleted when RAM is cleared.

Editing CONFIG.SYS with an External Editor

You can create and edit the CONFIG.SYS files of Omni 37xx applications through an IBM PC-compatible computer when you download files to the terminal. For more information on editing an application's CONFIG.SYS file, refer to the *VeriCentre Reference Manual*, the *Verix Operating System Programmer's Manual* (VPN 19733), or contact your local VeriFone representative.

For more information about using VeriCentre Download Management Module in client-server installations, please contact your local VeriFone representative.

System Mode Menu 4

In this menu you can view the error log and perform application debugging operations.

Table 11 System Mode Menu 4

Display	Action
SYS MODE MENU 4 REMOTE DIAGS F2 ERROR LOG F3 DEBUGGER F4 ↑ ↓	To initiate remote diagnostics, select REMOTE DIAGS F2. To view the error log screens, select ERROR LOG F3. To start an application's debug monitor, select DEBUGGER F4. To return to the previous system mode menu, press the PF1 key; to toggle through to SYS MODE MENU 5, press the PF2 key; to return immediately to SYS MODE MENU 1, or to quit any operation within this menu, press the cancel key.

Table 11 System Mode Menu 4

Display	Action
REMOTE DIAGS F2	
LOAD TERMINAL MANAGEMENT AGENT	REMOTE DIAGS: This function is reserved for VeriFone use. To return to the previous system mode menu, press the PF1 key; to return immediately to SYS MODE MENU 1, or to quit any operation within this menu, press the cancel key.
ERROR LOG F3	
SYS MODE ERR LOG TYPE 0004 FRAME 00040040 03DE0000 00000000 00001002 ↓	The first filename is shown on line two. The next line shows the file size in bytes, the file date, and the authentication status of the file. The 'A' means the file was authenticated by VeriShield. Unauthenticated files do not have the 'A'. Up to three files are shown on each screen. Pressing the ' ' key shows the next screen of filenames, if any. Pressing ' ' shows the previous screen of filenames, if any.
SYS MODE ERR LOG USP 00C04DDC TCB 00072CEC TIME 030806025642 ↑	This screen displays the following: USP (User Stack Pointer) TCB (Task Control Block) TIME (binary-coded, decimal system, clock time of the error in the format *yymmddhhmmss*, where *yy* = year, *mm* = month, *dd* = day, *hh* = hour, *mm* = minute, and *ss* = second) After taking desired notes, press the PF1 key to view the previous screen or press the cancel key to return to the main menu.
DEBUGGER F4	
SYS MODE FILE FILE GROUP _1	To search for keyed records in a particular file group, type the appropriate group number and press [↵]. If you cannot locate a particular keyed record, it may be stored in another file group. To search for keyed records in another file group, return to the main menu by pressing the cancel key, then type the appropriate group number and press [↵]. To correct a mistake, press [←] to delete the number, and type the new entry.

Table 11 System Mode Menu 4

Display	Action
SYSTEM MODE FILE GROUP nn PASSWORD ----------	To continue, enter the required password. If you enter an incorrect password, the following message appears: SYS MODE PASSWORD PLEASE TRY AGAIN Press [↵]. Verify your password and re-enter it. Invoking the Debugger starts the application program's debug monitor, if installed, on the selected file group. The *Verix Operating System Programmer's Manual* (VPN 19733) fully documents debug operations. For more information on debugging your terminal, contact your terminal supplier.

System Mode Menu 5

In this menu you can test the display panel, keyboard, and magnetic stripe card reader.

Table 12 System Mode Menu 5

Display	Action
SYS MODE MENU 5 SCREEN DIAG F2 KEYBOARD DIAG F3 MAG CARD DIAG F4 ↑ ↓	To test the display panel, select SCREEN DIAG F2. To test the keyboard, select KEYBOARD DIAG F3. To test the magnetic card reader, select MAG CARD DIAG F4. To return to the previous system mode menu, press the PF1 key; to toggle through to SYS MODE MENU 6, press the PF2 key; to return immediately to SYS MODE MENU 1, or to quit any operation within this menu, press the cancel key.
SCREEN DIAG F2	
(solid test pattern)	When you select F2, you should see a completely dark screen. Press [↵] to completely clear the screen. To stop the test and return to the main menu, press the cancel key.
KEYBOARD DIAG F3	
SYS MODE KBD TEST KEYCODE nn	This screen displays the decimal ASCII keycode for each key you press. The value displayed corresponds to the actual key pressed. Other values assigned to keys (for example, "Q", "Z", and "." are assigned to [1]) are software dependent. To test the keyboard, press some keys and check that they match their ASCII keycodes (for example, [1] displays keycode 31). For more ASCII keycodes, refer to the ASCII table in Appendix B. To stop the test and return to the main menu, press either the cancel key or [↵].

Table 12 System Mode Menu 5

Display	Action
MAG CARD DIAG F4	
SYS MODE TRK 1:VALID DATA TRK 2:VALID DATA TRK 3:VALID DATA	To test the magnetic-stripe card reader, swipe a magnetic-stripe card through it. A successful test displays VALID DATA for each track that read valid data. An error generates one of the following error messages for each track with an error: • NO DATA • NO START • NO END • LRC ERR • PARITY ERR • REVERSE END For more information about magnetic card error messages, refer to the *Verix Operating System Programmer's Manual* (VPN 19733). To stop the test and return to the main menu, press the cancel key.

System Mode Menu 6

In this menu you can run integrated PIN pad (IPP) diagnostics, check the IPP key loading mode, display printer information, and run printer tests.

Table 13 System Mode Menu 6

Display	Action
SYS MODE MENU 6 IPP DIAG F2 IPP KEY LOAD F3 PRINTER DIAG F4 ↑ ↓	To test the IPP, select IPP DIAG F2. To test the IPP key load, select IPP KEY LOAD F3. To run printer diagnostics and test the printer, select PRINTER DIAG F4. To return to the previous system mode menu, press the PF1 key; to return immediately to SYS MODE MENU 1, or to quit any operation within this menu, press the cancel key.
IPP DIAG F2	
INTERNAL PIN PAD MEMORY TEST PASSED IPP6 0PGP021 12/99 B6 SN: 00000000000000000 BAUD: 1200RESET F3 MODE: VISA EXIT F4	When you select F2, the INTERNAL PIN PAD screen appears and the diagnostic test begins. The firmware version and download date, IPP serial number, baud rate, and mode display. To reset the IPP, press F3; to exit the test and return to SYS MODE MENU 6, press F4 or the cancel key.

Table 13 System Mode Menu 6

Display	Action
IPP KEY LOAD F3	
INTERNAL PIN PAD KEY LOADING MODE BYTES SENT 0 BYTES RCVD 0 END F4	Select this mode when using SecureKit or programming from your PC to inject keys into your terminal. In this mode, a pipe is opened through COM1 to the IPP to allow key loading. Press the cancel key to stop the key load session; press F4 when finished with the key load.
PRINTER DIAG F4	
Printer ID M Version 0SAT023 Status 22 Test F3 Paper Feed F4	When you select F4, the firmware ID and version, and the printer status appear. Press F3 to run the printer test. A print sample begins that uses approximately 30.5 cm (12”) of paper. This allows you to test the print quality and adjust your code for print optimization. See the *Verix Operating System Programmer’s Manual* (VPN 19733) for specifics on application development and the internal thermal printer. Press F4 to run approximately 5 cm (2”) of paper through the printer without printing. To exit this screen, press the cancel key.

System Mode Menu 7

In this menu, you can view file information for the RAM and Flash directories in each file group.

Table 14 System Mode Menu 7

Display	Action
SYS MODE MENU 7 RAM DIRECTORY F3 FLASH DIRECTORY F4 ↑	To test the IPP, select IPP DIAG F2. To test the IPP key load, select IPP KEY LOAD F3. To run printer diagnostics and test the printer, select PRINTER DIAG F4. To return to the previous system mode menu, press the PF1 key; to return immediately to SYS MODE MENU 1, or to quit any operation within this menu, press the cancel key.

Table 14 System Mode Menu 7

Display	Action
RAM DIRECTORY F3	
SYS MODE FILE FILE GROUP _1	Type the number of the file group (1 for the primary application; between 1–15 for other applications) and press [↵] to view a list of files in the flash directory. To search for files in a particular file group, type the appropriate group number and press [↵]. If you cannot locate a particular file, it may be stored in another file group. To search for files in another file group, return to the main menu by pressing the cancel key, then type the appropriate group number and press [↵]. To correct a mistake, press [←] to delete the number, and type the new entry.
SYSTEM MODE FILE GROUP nn PASSWORD ----------	To continue, enter the required password. If you enter an incorrect password, the following message appears: SYS MODE PASSWORD PLEASE TRY AGAIN Press [↵]. Verify your password and re-enter it.
RAM DIRECTORY G 1 O37XXF.OUT 46082 09/27/03 A TEST2250.VFT 784 09/27/03 - CONFIG.SYS 66 09/27/03 -	The first filename is shown on line two. The next line shows the file size in bytes, the file date, and the authentication status of the file. Authentication status: • 'A' means the file was authenticated by VeriShield. • '-' Unauthenticated files do not have the 'A'. To scroll through keyed records, press either the PF1 or the PF2 key, below the Left and Right arrows respectively (if displayed), as needed. To exit this screen, press the cancel key. You are returned to SYS MODE MENU 7.
FLASH DIRECTORY F4	
SYS MODE FILE FILE GROUP _1	Type the number of the file group (1 for the primary application; between 1–15 for other applications) and press [↵] to view a list of files in the flash directory. To search for files in a particular file group, type the appropriate group number and press [↵]. If you cannot locate a particular file, it may be stored in another file group. To search for files in another file group, return to the main menu by pressing the cancel key, then type the appropriate group number and press [↵]. To correct a mistake, press [←] to delete the number, and type the new entry.

Table 14 System Mode Menu 7

Display	Action

`SYSTEM MODE FILE`
`GROUP nn PASSWORD`
`----------`
	To continue, enter the required password. If you enter an incorrect password, the following message appears:
	`SYS MODE PASSWORD`
	`PLEASE TRY AGAIN`
	Press [↵]. Verify your password and re-enter it.

`FLASH DIRECTORY G 3`
`A.OUT`
`1234567 09/27/03 A`
`CARDDATA.DAT`
`9876543 09/27/03 -`
	The first filename is shown on line two. The next line shows the file size in bytes, the file date, and the authentication status of the file.
	Authentication status:
	• 'A' means the file was authenticated by VeriShield.
	• '-' Unauthenticated files do not have the 'A'.
	To scroll through keyed records, press either the PF1 or the PF2 key, below the Left and Right arrows respectively (if displayed), as needed.
	To exit this screen, press the cancel key. You are returned to `SYS MODE MENU 7`.

CHAPTER 5

File Authentication

This chapter discusses VeriShield's *file authentication* security architecture.

- Overviews the VeriShield file authentication module, and the organizational infrastructure that supports it. See Introduction to File Authentication.
- Explains how the file authentication process may affect the tasks normally performed by application programmers, terminal deployers, site administrators, or by entities authorized to download files to an Omni 37xx terminal. See File Authentication and the File System.
- Describes how to use the file signing utility, FILESIGN.EXE, to generate the signature files that are required to perform downloads and authenticate files on the Omni 37xx terminal. See FILESIGN.EXE File Signing Tool.

In Chapter 6, the topic of file authentication is also discussed in the context of specific file download procedures.

Introduction to File Authentication

The Omni 37xx terminal has a new type of security architecture, developed by VeriFone. This architecture, called VeriShield, has both physical and logical components. The logical security component of the VeriShield architecture, which is part of the terminal's operating system software, is called the file authentication module, or simply, file authentication.

File authentication is a secured process for authenticating files using digital signatures, cryptographic keys, and digital certificates. This process makes it possible for the sponsor of an Omni 37xx terminal to logically secure access to the terminal by controlling who is authorized to download application files to that terminal. It proves and verifies the, file's origin, sender's identity, and integrity of the file's information.

The VeriFone Certificate Authority

To manage the tools and processes related to the file authentication module of the VeriShield security architecture, VeriFone has established a centralized VeriFone Certificate Authority, or *VeriFone CA*. This agency is responsible for managing keys and certificates. The VeriFone CA uses an integrated set of software tools to generate and distribute digital certificates and private cryptographic keys to customers who purchase Omni 37xx terminals.

Special Files Used in the File Authentication Process

The following specially formatted files support the file authentication process:

- A **digital certificate** is a digital, public document used to verify the signature of a file.

- A **digital signature** is a piece of information based on both the file and the signer's **private cryptographic key**. The file sender digitally *signs* the file using a private key. The file receiver uses a digital certificate to verify the sender's digital signature.
- **Signer private keys** (*.key files) are securely conveyed to clients on smart cards. The secret passwords required by clients to generate signature files, using signer private keys, are sent as PINs over a separate channel such as registered mail or encrypted E-mail.

Some files, such as private key files, are encrypted and password-protected for data security. Others, such as digital certificates and signature files, do not need to be kept secure to safeguard the overall security of VeriShield.

Within the FILESIGN.EXE tool, you can recognize the special file types that support the file authentication process by their filename extensions:

Table 14 FILESIGN.EXE tool Filename Extensions

File Type	Extension
Signature	*.p7s
Private key	*.key
Digital certificate	*.crt

All digital certificates are generated and managed by the VeriFone CA, and are distributed on request to Omni 37xx clients — either internally within VeriFone or externally to sponsors.

All certificates that are issued by the VeriFone CA for the Omni 37xx platform, and for any VeriFone platform with the VeriShield security architecture, are hierarchically related. That is, a lower-level certificate can only be authenticated under the authority of a higher-level certificate.

The security of the highest-level certificate, called the *platform root certificate*, is tightly controlled by VeriFone.

The required cryptographically-related private keys that support the file authentication process are also generated and distributed by the VeriFone CA.

Certificates Contain Keys That Authenticate Signature Files

- **Sponsor certificate:** Certifies a client's sponsorship of the terminal. It does not, however, convey the right to sign and authenticate files. To add flexibility to the business relationships that are logically secured under the file authentication process, a second type of certificate is usually required to sign files.

  A sponsor certificate is authenticated under a higher-level system certificate, called the *application partition certificate*.

NOTE

Only one sponsor certificate is permitted per terminal.

- **Signer certificate:** Certifies the right to sign and authenticate files for terminals belonging to the sponsor.

  A signer certificate is authenticated under the authority of a higher-level client certificate (the sponsor certificate).

The required sponsor and signer certificates must either have been previously downloaded and authenticated on the terminal, or they must be downloaded together with the new signature files and target files for them to authenticate.

Signer Private Keys Are Issued to Secure the File Signing Process

Signer private keys are loaded onto a smart card. This smart card is securely delivered to the business entity that the terminal sponsor has authorized to sign, download, and authenticate applications to run on the sponsor's terminal.

The VeriFone CA can also issue additional sets of sponsor and signer certificates, and signer private keys to support multiple sponsors and multiple signers for a specific platform.

To establish the logical security of applications to download to an Omni 37xx terminal, the designated signer uses the signer private key issued them by the VeriFone CA as a required input to the file signing tool, FILESIGN.EXE. Every signature file contains information about the signer private key used to sign it.

When a signature file generated using a signer private key downloads to the Omni 37xx terminal, if it is successfully authenticated depends on whether the signer private key used to sign the target file matches the signer certificate stored in the terminal's certificate tree.

How File Authentication Works

File authentication consists of three basic processes:

1. **Development:** The file signing software tool FILESIGN.EXE creates a signature file for each application file to authenticate.
2. **Pre-deployment:** An optimal certificate structure is determined, and the necessary certificates and keys created.
3. **Deployment:** The development and pre-deployment processes, once complete, are used in combination to prepare a terminal for deployment.

Development Process

In this process:

1. The application developer creates an application file.
2. The developer assigns a name to the application file.

3. The application file becomes a required input for the FILESIGN.EXE tool (included in the SDK).
4. The default certificate (K2SIGN.CRT) and default key (K2SIGN.KEY) included in the SDK are inputs for the FILESIGN.EXE tool.
5. Using the application file, default certificate, and default key, FILESIGN.EXE creates a signature file (*.p7s).
6. The signature file and the original application file are loaded into a development terminal, where the following actions occur:
   a. The terminal's operating system searches for signature files.
   b. When a signature file is found, the operating system then searches for a matching application file.
   c. When a matching application file is found, the operating system compares the signature file's signature against the values stored in the application file's calculated signature.
   d. If these values match, the two files are authenticated, and the ATTR_NOT_AUTH bit is set to 0.
7. The application file is tested and debugged.
8. After the application file is fully debugged, it becomes an input for the deployment process.

Figure 14 illustrates the development process.

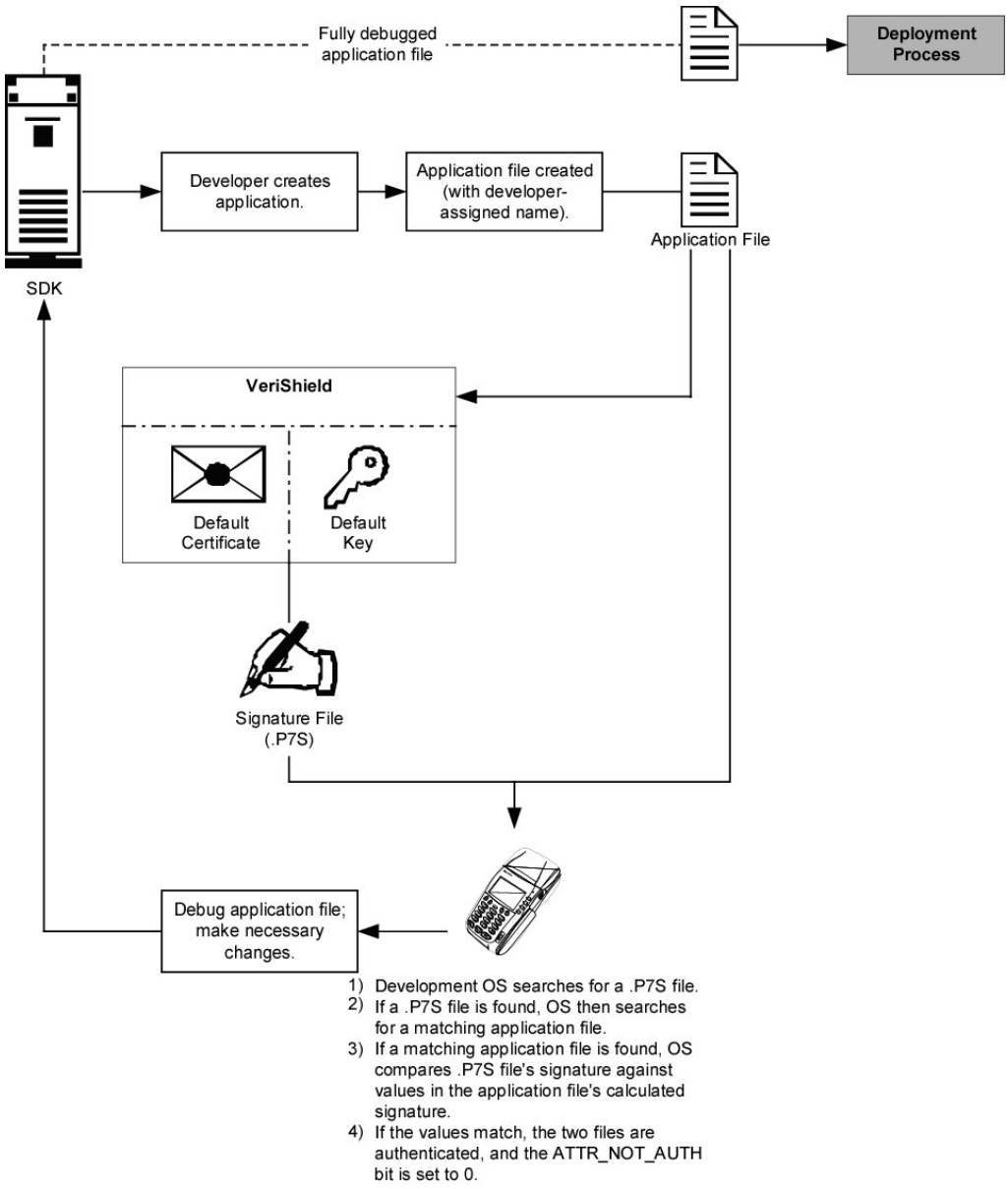

Fully debugged application file
Deployment Process
SDK
Developer creates application.
Application file created (with developer-assigned name).
Application File
VeriShield
Default Certificate
Default Key
Signature File (.P7S)
Debug application file; make necessary changes.
1) Development OS searches for a .P7S file.
2) If a .P7S file is found, OS then searches for a matching application file.
3) If a matching application file is found, OS compares .P7S file's signature against values in the application file's calculated signature.
4) If the values match, the two files are authenticated, and the ATTR_NOT_AUTH bit is set to 0.

Figure 14 The Development Process

Pre-Deployment Process

In this process:

1. A sponsor goes to the VeriFone CA Web site and requests certificates for deployment terminals.
2. Based on information provided by the sponsor through the VeriFone CA Web site, the VeriFone CA determines the required certificate structure.
3. VeriFone CA generates the following items for the sponsor:
   a. Smart card containing a set of certificates and keys.
   b. Smart card PIN.

4 VeriFone CA sends the smart card and smart card PIN to the sponsor.

5 The sponsor uses the smart card and smart card PIN as inputs for the deployment process.

Refer to Figure 15 illustrates the pre-deployment process.

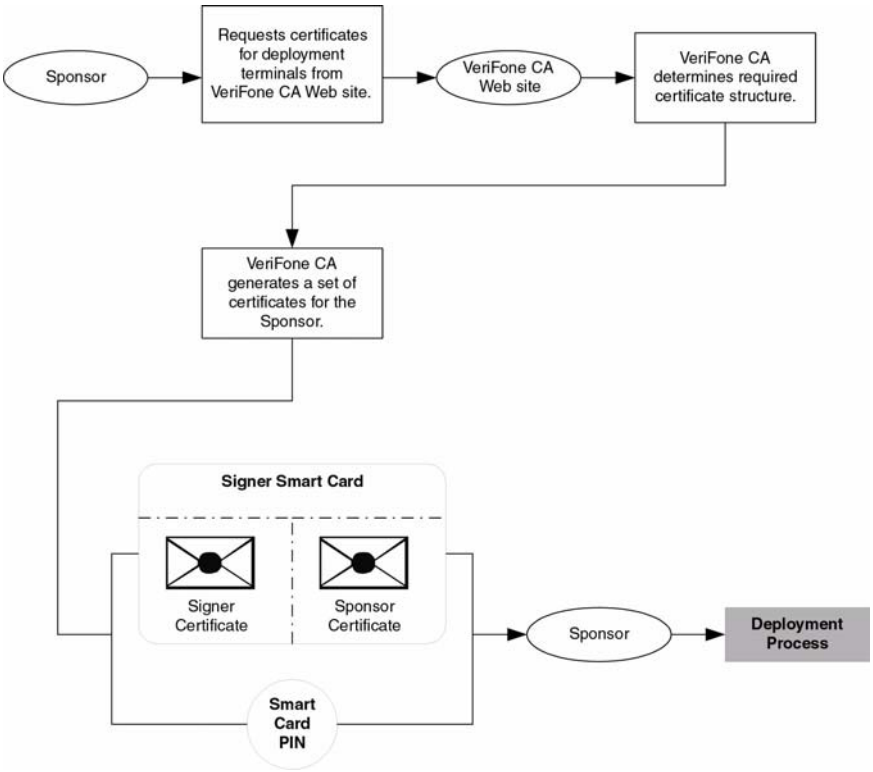

Sponsor
Requests certificates for deployment terminals from VeriFone CA Web site.
VeriFone CA Web site
VeriFone CA determines required certificate structure.
VeriFone CA generates a set of certificates for the Sponsor.
Signer Smart Card
Signer Certificate
Sponsor Certificate
Sponsor
Deployment Process
Smart Card PIN

Figure 15 The Pre-Deployment Process

Deployment Process

In this process:

1 The sponsor provides the application file (from the development process) and the smart card and smart card PIN (from the pre-deployment process) as inputs to VeriShield.

2 VeriShield extracts the signer key, signer certificate, and sponsor certificate from the smart card.

3 VeriShield uses the extracted data, along with the application file, to create a signature file (*.p7s).

4 VeriShield creates files suitable for downloading from the extracted smart card data.

5 The signature file, the application file, and the extracted signer and sponsor certificates are downloaded into a deployment terminal, where the following actions occur:

   a The terminal's operating system searches for signature files.

b. If a signature file is found, the operating system then searches for a matching application file.

c. If a matching application file is found, the operating system compares the signature file's signature against the values stored in the application file's calculated signature.

d. If the values match, the two files are authenticated and the ATTR_NOT_AUTH bit is set to 0.

6. Each successfully authenticated executable application file is allowed to run on the terminal (otherwise, the executable remains stored in the terminal memory but is not allowed to run).

Figure 16 illustrates the deployment process.

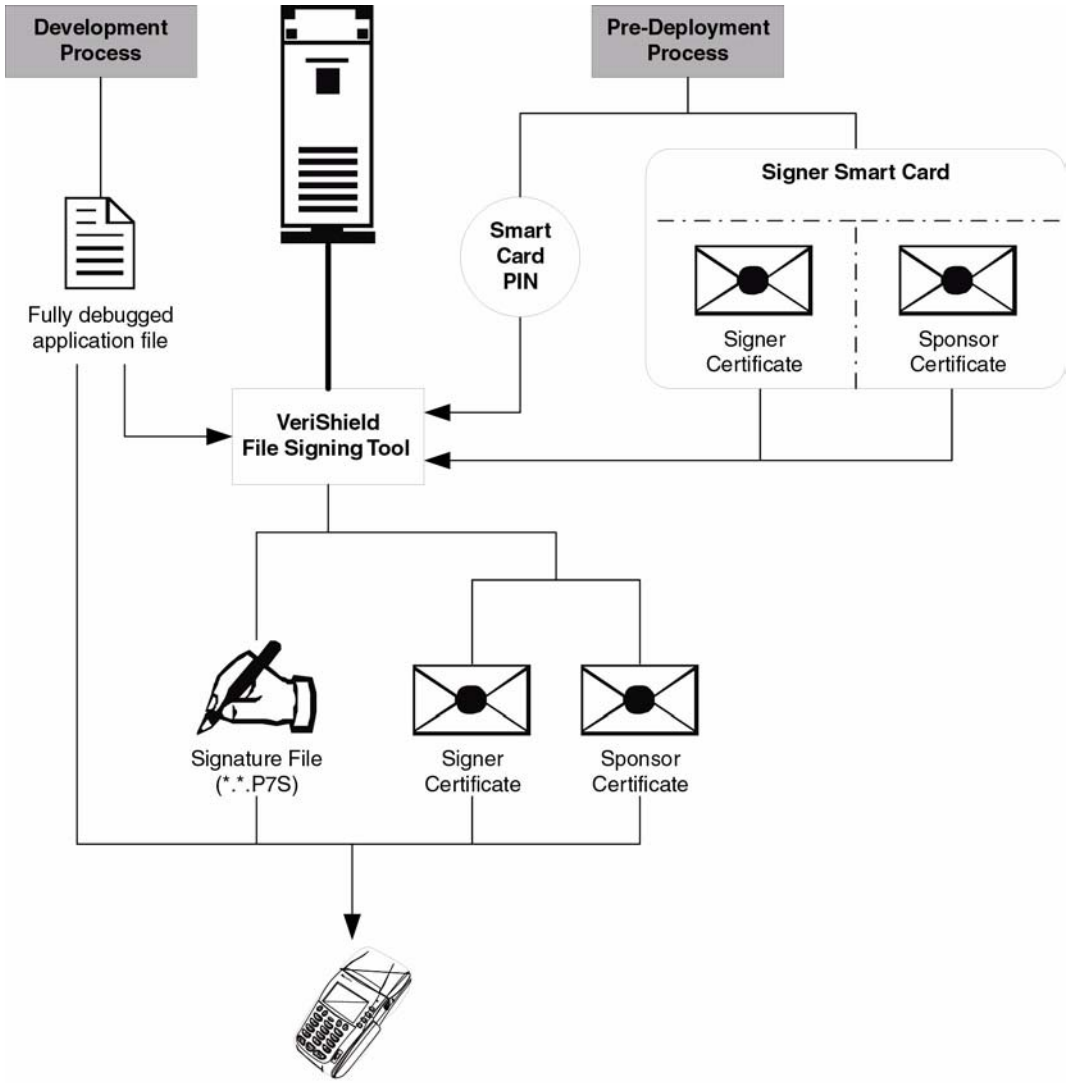

Development Process
Pre-Deployment Process
Signer Smart Card
Smart Card PIN
Fully debugged application file
Signer Certificate
Sponsor Certificate
VeriShield File Signing Tool
Signature File (*.*.P7S)
Signer Certificate
Sponsor Certificate
1) Development OS searches for a *.*.P7S file.
2) If a *.*.P7S file is found, OS then searches for a matching application file.
3) If a matching application file is found, OS compares *.*.P7S file's signature against values in the application file's calculated signature.
4) If the values match, the two files are authenticated, and the ATTR_NOT_AUTH bit is set to 0.

Figure 16 The Deployment Process

Planning for File Authentication

File authentication is an integral part of every Omni 37xx terminal. To safeguard the terminal's logical security, the file authentication module requires that *any executable code file* must be successfully authenticated before the operating system allows it to execute on the terminal.

Authentication Requirements for Specific File Types

For the purposes of file authentication, executable code files include two file types that can be recognized by their filename extensions:

Table 15 Executable File Extensions

File Type	Extension
Compiled and linked application files	*.out
Global function libraries	*.lib

Depending on the logical security requirements of specific applications, other types of files used by an application (that is, non-executable files) also need to be authenticated:

- Data files (*.dat) that contain sensitive customer information or other data that needs to be secure
- Font files (*.vft or *.fon) that may need to be secure to prevent unauthorized text or messages from being displayed on the terminal screen
- Any other type of file used by an application and that the application designer wishes to logically secure using file authentication requirements

Decide Which Files to Authenticate in a Specific Application

The first step in the file authentication process is to determine which files must be authenticated for an application to meet its design specifications for logical security under the VeriShield security architecture.

In most cases, application designers make these decisions based on specifications provided by the terminal sponsor. Which files to authenticate can be completely transparent to the person or business entity responsible for signing, downloading, and authenticating an application prior to deployment.

How (and When) Signature Files Authenticate Their Target Files

Signature files are usually downloaded together with their target application files in the same data transfer operation. This recommended practice lets you specify and confirm the logical security status of the Omni 37xx terminal each time you perform an application download.

When the file authentication module detects a new signature file after a terminal restart, it locates and attempts to authenticate the target file that corresponds to the new signature file.

It is not mandatory to always download a signature file at the same time as its target application file. For example, you can download the corresponding signature file in a separate operation. A non-authenticated application can reside in the terminal memory, but is not authenticated or allowed to run on the terminal until the signature files for the application executable files are processed by the file authentication module after a subsequent download procedure and terminal restart.

Determine Successful Authentication

To ensure the Omni 37xx terminal's logical security, never assume that a target file was authenticated simply because it downloaded to the Omni 37xx terminal together with its signature file.

There are several ways to ensure a target file successfully authenticated after a download:

- **Confirm all downloaded executable files run.** If an executable code file is not successfully authenticated, the operating system does not allow it to execute and run, either following the initial download or on subsequent terminal restarts. The effect of this rule depends on whether or not *all* executable files successfully authenticated:
  - If the executable file that failed to authenticate is the main application (*.out) specified in the CONFIG.SYS *GO variable, the main application is not allowed to run.
  - If the executable that failed to authenticate is a secondary executable (*.out) or shared library (*.lib) used by the main application, the CONFIG.SYS *GO application executes and runs until it issues a function call to that library. When the main application attempts to access a non-authenticated executable, the main application may crash.
- **Visually (and audibly) confirm file authentication during the process.** When the file authentication module is invoked at terminal restart and detects a new signature file, it displays status information on screen indicating success or failure of the authentication of each target file based on its corresponding signature file. (A similar status display also appears on screen when you download digital certificates.)

  You can watch the screen display following the download to see if a specific target file fails to be authenticated. If this happens, FAILED displays on screen for five seconds below the filenames of the target and signature files, and the terminal beeps as an alert.

  An application program can issue a function call to read the ATTR_NOT_AUTH bit's current value for all relevant files to verify that were successfully authenticated. If the ATTR_NOT_AUTH bit's binary value is 1, the file did *not* authenticate; if 0, the file did authenticate.

For non-executable files, it is the application's responsibility to confirm that all of the files it uses successfully authenticated on download completion, and when the application executes the first time following a restart.

NOTE

Because the application is responsible for verifying data files and prompt files, it is recommended that each application check the ATTR_NOT_AUTH bit of all relevant files on restart.

NOTE

Each successfully authenticated file is also write-protected. That is, the file's read-only attribute is set. If the read-only file is removed or if the file is modified in any way while stored in the terminal, the ATTR_NOT_AUTH bit is automatically set to 1. If the modified file is an executable, it is no longer allowed to run.

Digital Certificates and the File Authentication Process

The file authentication module always processes certificates before it processes signature files. Digital certificates (*.crt files) generated by the VeriFone CA have two important functions in the file authentication process:

- They define the rules for file location and usage (for example, the valid file group, replaceable *.crt files, parent *.crt files, whether child *.crt files can exist, and so on).
- They convey the public cryptographic keys generated for terminal sponsors and signers that are the required inputs to the file signing tool, FILESIGN.EXE, to verify file signatures.

Hierarchical Relationships Between Certificates

All digital certificates are hierarchically related to one another. Under the rules of the certificate hierarchy managed by the VeriFone CA, a lower-level certificate must always be authenticated under the authority of a higher-level certificate. This rule ensures the overall security of VeriShield.

To manage hierarchical relationships between certificates, certificate data is stored in terminal memory in a special structure called a *certificate tree*. New certificates are authenticated based on data stored in the current certificate tree. The data from up to 21 individual related certificates (including root, OS, and other VeriFone-owned certificates) can be stored concurrently in a certificate tree.

This means that a new certificate can only be authenticated under a higher-level certificate *already resident* in the terminal's certificate tree. This requirement can be met in two ways:

- The higher-level certificate may have already been downloaded to the terminal in a previous or separate operation.
- The higher-level certificate can be downloaded together with the new certificate as part of the same data transfer operation.

A development set of higher-level certificates is downloaded into each Omni 37xx terminal at manufacture. When you take a new Omni 37xx terminal out of its shipping carton, certificate data is already stored in the terminal's certificate tree. In this just-out-of-the-box condition, the Omni 37xx terminal is called a *development terminal*.

Typically, a sponsor requests an additional set of digital certificates from the VeriFone CA to establish sponsor and signer privileges. This additional set of certificates are then downloaded to the Omni 37xx terminal when the terminal is being prepared for deployment. When this procedure is complete, the Omni 37xx terminal is called a deployment terminal.

Add New Certificates

When you add a new certificate file to an Omni 37xx terminal, the file authentication module detects it by filename extension (*.crt). On restart, the terminal then attempts to authenticate the certificate under the authority of the resident higher-level certificate stored in the terminal's certificate tree or one being downloaded with the new certificate.

In a batch download containing multiple certificates, each lower-level certificate must be authenticated under an already-authenticated, higher-level certificate. Whether or not the data a new certificate contains is added to the terminal's certificate tree depends on if it is successfully authenticated. The following points explain how certificates are processed:

- If a new certificate is successfully authenticated, the information it contains is automatically stored in the terminal's certificate tree. The corresponding certificate file (*.crt) is then deleted from that file group's RAM.
- If the relationship between the new certificate and an existing higher-level certificate cannot be verified, the authentication procedure for the new certificate fails. In this case, the certificate information is *not* added to the certificate tree and the failed certificate file (usually ~400 bytes) is retained in application memory.

Development Terminals

A development terminal is an Omni 37xx terminal still maintaining the original factory set of certificates in its certificate tree. This set of certificates includes several higher-level system certificates and a special client certificate called a default signer certificate (see Figure 17).

In the development terminal, the level of logical security provided by the file authentication module is minimal, even though applications must still be signed and authenticated before they can run on the terminal. In most application development and test environments, tight security is not required, and the flexibility offered by the Omni 37xx development terminal is more important.

NOTE

With the factory set of certificates stored in the terminal memory, *anyone* who has the Omni 37xx SDK and included file signing tool, FILESIGN.EXE, can generate valid signature files for downloading and authenticating files on the Omni 37xx platform.

Deployment Terminals

While the application development process is being completed and while the new application is being tested on a development terminal, a sponsor can order specific sponsor and signer certificates from the VeriFone CA to use to logically secure sponsor and signer privileges when the Omni 37xx terminal is prepared for deployment.

Customer-specific sponsor and signer certificates are usually downloaded to an Omni 37xx terminal as part of the standard application download procedure performed by a deployment service. In this operation, the new sponsor and signer certificates replace the development sponsor certificate that is part of the factory set of certificates, as shown in Figure 17.

When the sponsor and signer certificates are downloaded and successfully authenticated, the terminal is ready to deploy.

Ultimately, it is the sponsor's decision how to implement the logical security provided by file authentication on a field-deployed terminal. Additional certificates can be obtained from the VeriFone CA any time, to implement new sponsor and signer relationships in deployment terminals.

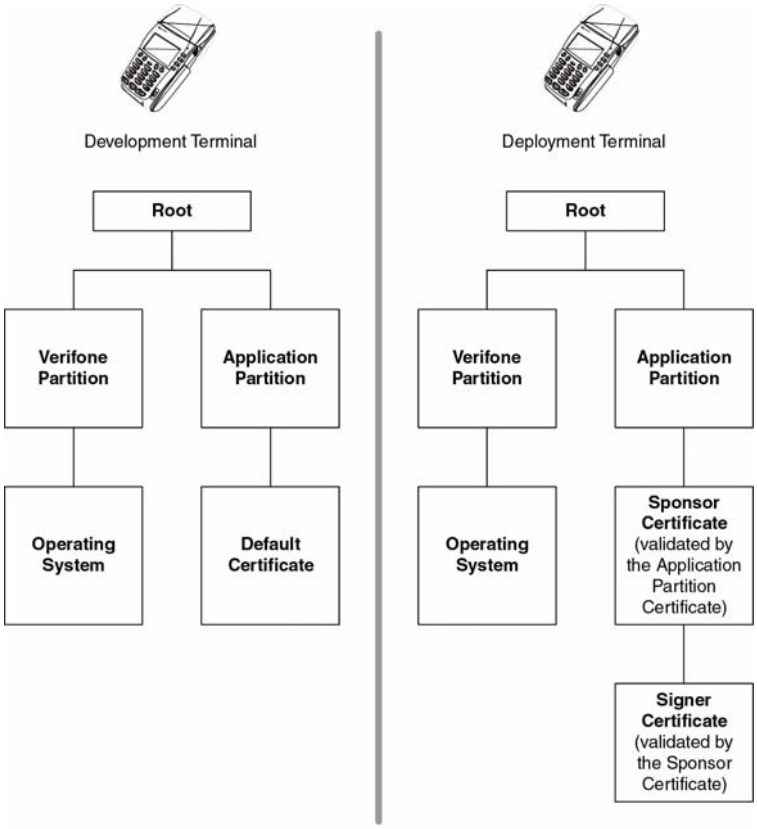


Figure 17 Certificate Trees in Development and Deployment Terminals

Permanency of the Certificate Tree

The data contained in a digital certificate is stored in the terminal's certificate tree when the certificate is authenticated, and the certificate file itself is erased from RAM.

The certificate tree file is stored in a reserved area of non-volatile memory and is therefore relatively permanent. New certificate data can be added to the existing certificate tree (up to a maximum of 21 certificates).

Required Inputs to the File Signing Process

The required inputs to the file signing process are somewhat different for development terminals than deployment terminals. The significant differences shown in Table 16.

Table 16 Differences Between Required Inputs

Development Terminals	Deployment Terminals
Manufacturing inputs to the file signing process are included, together with the file signing tool, FILESIGN.EXE, in the Omni 37xx SDK. These inputs make it possible for anyone who has the Omni 37xx SDK to sign and authenticate files.	The required inputs to FILESIGN.EXE must be obtained from the VeriFone CA to logically secure the sponsor and signer privileges for the terminal.
The following two factory inputs are required for the file signing process, in addition to the application files you want to sign and authenticate: • **Default signer certificate**, with the filename K2SIGN.CRT • **Default signer private key**, with the filename K2SIGN.KEY	The following three unique inputs, which are issued at customer request by the VeriFone CA, are required for the file signing process, as well as the application files you want to sign and authenticate: • **Customer signer certificate:** This unique certificate is a required input for FILESIGN.EXE and must be downloaded to the terminal along with the signature files and target application files to authenticate, unless already downloaded to the terminal in a previous operation. • **Customer signer private key:** The VeriFone CA issues this unique, encrypted private key file (*.key) to an authorized signer at the sponsor's request. The signer private key is a required input to FILESIGN.EXE, but does not have to be downloaded to the terminal. • **Customer signer PIN:** The VeriFone CA issues this unique password to an authorized signer at the sponsor's request. The customer signer password is a required input to FILESIGN.EXE, but it does not have to be downloaded to the terminal.
Note: A default signer password is not a required entry when using FILESIGN.EXE to sign files for an Omni 37xx development terminal.	**Note:** The customer sponsor certificate, which authenticates the customer signer certificate, is usually downloaded to the terminal with the customer signer certificate, but it is not a required FILESIGN.EXE input when signing files to be downloaded to, and authenticated on, a deployment terminal.

Replace a Sponsor Certificate

A sponsor may need to clear the current sponsor certificate from a terminal so that a new sponsor can load certificates and applications. To do this, the original sponsor must order a "clear" smart card from the VeriFone CA. The clear smart card is specific to the requesting sponsor. It restores a deployment terminal to the development state (refer to Figure 18) by:

- Deleting the current sponsor and signer certificates from the terminal's application partition.
- Restoring the default certificate to the terminal's application partition.

NOTE

The process for replacing a signer certificate is the same as for replacing a sponsor certificate.

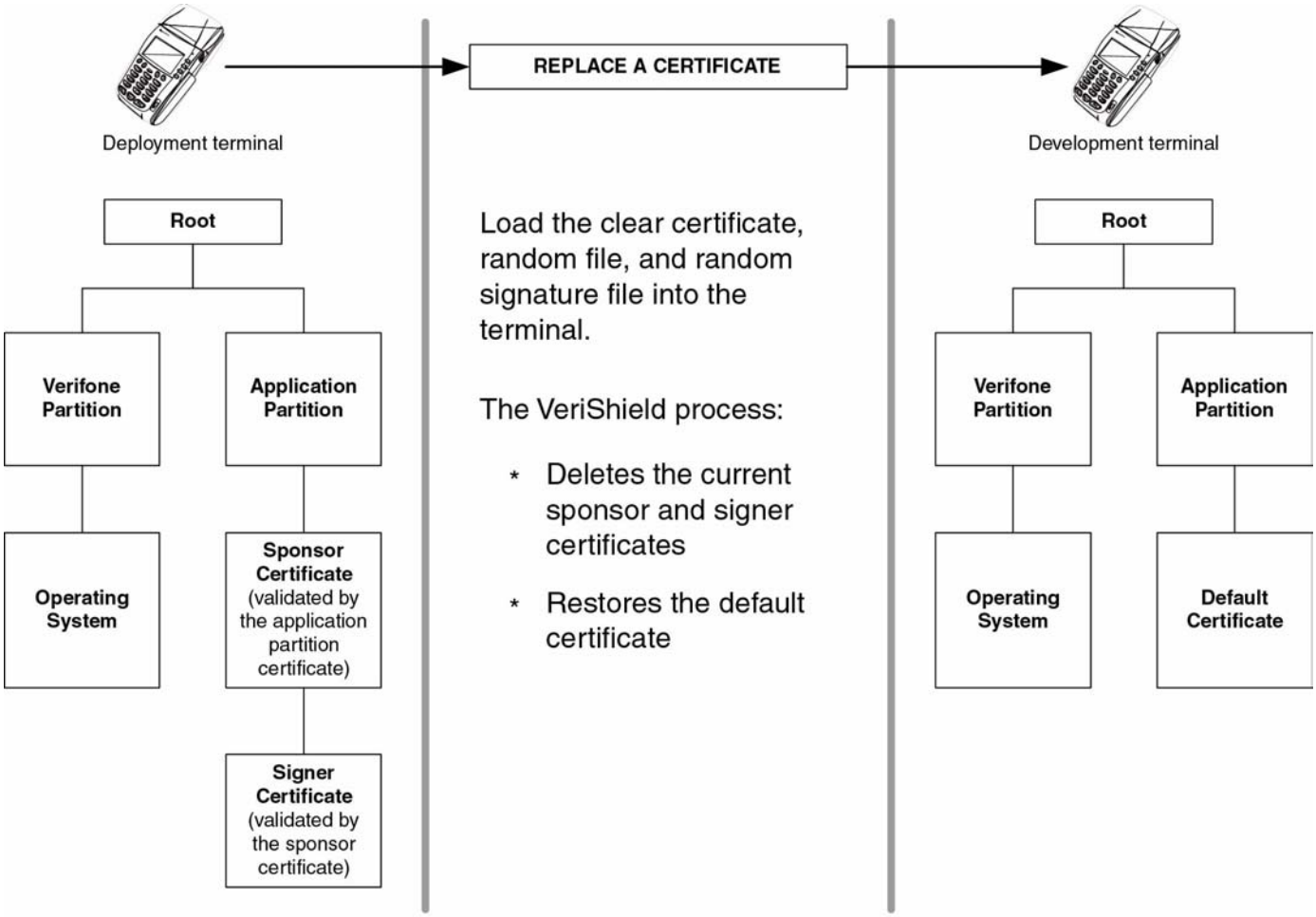


Figure 18 Certificate Replacement Process

File Authentication and the File System

Application Memory Logically Divided Into File Groups

The memory of an Omni 37xx terminal is logically divided into two main areas, or partitions: One partition is for the operating system and the other partition is reserved for applications. The application partition is further divided into sub-partitions. These sub-partitions are called file groups or GIDs.

This system of partitions and sub-partitions makes it possible to store multiple applications in terminal memory and prevent these applications from overlapping or otherwise interfering with each other's operation.

There are a total of 16 file groups (Figure 19). Group 0 is the name of the operating system partition. Group 1 is reserved for the main application. Groups 2–14 are available for related executable files or secondary applications. Group 15 is *open*, and used for shared files.

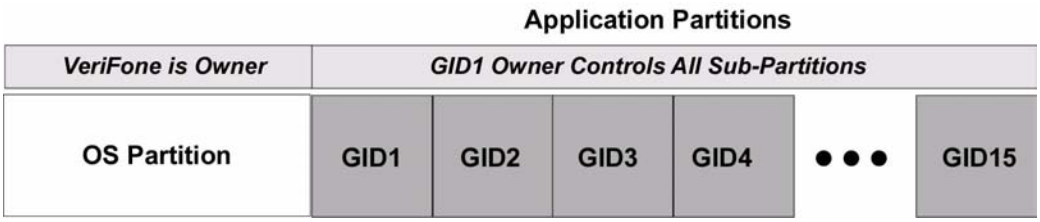


Figure 19 Omni 37xx Application Memory Partitions

NOTE

The Omni 37xx operating system only enforces the rule that the main application always be stored in GID1. You can, for example, store a shared library in any file group. Rules for Storing Applications in Specific File Groups states reasons to follow the guidelines previously described for storing applications and libraries in specific file groups.

Rules for Storing Applications in Specific File Groups

Here are some important Omni 37xx file system features, as they relate to storing application files in specific file groups, and how these features affect the file authentication process:

- Most applications consist of more than one executable. For *each* executable to run on the terminal, it must be signed and authenticated.
- Although not enforced by the operating system, it is recommended that only one application be stored per file group in the application partition. Any number of executable files can, however, be stored in a single file group.
- Using the CONFIG.SYS *GO variable, you can specify only one application to automatically execute following a download and terminal restart. The defined application is usually the main application stored in Group 1 and called from the *GO variable in the CONFIG.SYS file in GID1.
- The main application stored in GID1 can access files, secondary applications, or function libraries stored in *any* other file group.
- The application downloaded into GID1 is *always* the primary application for the terminal. This application is owned by the primary terminal sponsor (sponsor A) in cases where there are multiple sponsors.
- The Group 1 application controls any and all secondary applications stored in terminal memory. That is, a secondary application can only be invoked by a RUN command issued by the Group 1 application.
- An application stored in Groups 2–15 can *only* access files stored in its own file group and in Group 15. For example, an application authorized by the sponsor to be authenticated in Group 4 can only access files and libraries stored in Group 4 and Group 15.
- If multiple applications (main and secondary) are to run on the same terminal, each .OUT and/or shared library file must have its own matching signature file.

Because each application is responsible for verifying its own data and prompt files, the other application files should have their own matching signature files. The master .OUT file should validate that these additional signature files are authenticate before the signature files are used.

- If two or more applications are to run on the same terminal, the signature files for the respective applications must be downloaded, together with the corresponding target files, into the specific file group(s) for which the applications are authorized. If an application is downloaded into a group for which is it not authorized, file authentication for that application fails.

  If, for example, Application B is downloaded into GID4, where it is authorized to run, but the signature files for all Application B executable files are downloaded into GID7, file authentication for Application B fails and it is not allowed to run.

- Each certificate contains an attribute to verify if an application is valid for a particular group.

Authenticate Files Stored in the RAM or Flash of a File Group

All *.p7s files are loaded into RAM and contain flags that indicate if the file to verify is stored in flash or RAM. A signature file must know if its matching application file is stored in flash or RAM. If a signature file cannot locate its matching application file, the application file is not authenticated.

If the signature file authenticates its target file, and if the *FA variable is present in the CONFIG.SYS file of the target file group and is set to 1, the signature file is retained in memory and is automatically moved, if necessary, into the same file system as the target file it authenticates. That is, if the target file is stored in the flash, the signature file is also stored in the flash; if the target file is stored in RAM, the signature file is also stored in RAM.

If the signature file authenticates its target file and the *FA variable is present in the CONFIG.SYS file of the target file group and is set to 0, the signature file is erased when its target file is authenticated.

If you intend to perform back-to-back downloads, as described in Chapter 6, all signature files *must* be retained in the Omni 37xx terminal's application memory, together with the target application files they authenticate.

NOTE

To control if signature files are retained or deleted when they are processed by the file authentication module, you must use the protected CONFIG.SYS variable *FA as documented in the *Verix Operating System Programmer's Manual* (VPN 19733).

Restrictions on Downloading Different File Types

A typical application download includes a variety of different file types. There are the following restrictions on how you can download different kinds of files to the Omni 37xx terminal and how files are stored in the file system:

Table 17 Download File Extensions

File Type	Restriction
Certificate (*.crt)	*Must* be downloaded into the RAM of the target file group (GID1–GI15) selected in system mode.
Signature (*.p7s)	*Must* be downloaded into the RAM of the target file group (GID1–GID15) that you select in system mode.
Operating system	*Must* be downloaded into Group 1 RAM. When the OS files and related certificates and signature files are authenticated, they are automatically moved from Group 1 RAM into the Group 0 sub-partition, reserved for the operating system.

The normal size of a signature file is approximately 400 bytes. Depending on the application's size and on how memory space is allocated, the area available for storing multiple signature files must be carefully managed. The memory space required by a certificate file is also approximately 400 bytes, but certificate files are temporary. When a certificate is authenticated, the data it contains is copied to the certificate tree, and the certificate file is erased from the target file group's RAM.

FILESIGN.EXE File Signing Tool

To generate the signature files required for file authentication, you must sign all executable files and other files to be logically protected, using the FILESIGN.EXE software tool. This section discusses use of this tool, which is included in the Omni 37xx SDK.

The file signing tool, FILESIGN.EXE, generates a formatted file called a *signature* file, recognized by the filename extension *.p7s.

You can run FILESIGN.EXE on a host computer (PC) in DOS command-line mode, or invoke the program under Windows NT or Windows 95 and then use the FileSign dialog box to make the required entries.

NOTE

The file signing process for operating system files is done for Omni 37xx customers by the VeriFone CA. For operating system updates, VeriFone provides customers with a complete download package that includes all certificates and signature files required for authentication.

FILESIGN.EXE System Requirements

The FILESIGN.EXE tool requires one of the following computing environments:

- Windows NT, Version 4.0, SP5
- Windows 95, with Internet Explorer Version 5.0

The SP5 and Internet Explorer Version 5.0 software can be downloaded from the Microsoft Web site located at www.microsoft.com.

Operating Modes for FILESIGN.EXE

FILESIGN.EXE can run on the host computer in two user modes:

- **Command-line mode** (Windows PC DOS shell): Command-line mode is useful for application developers who perform batch file downloads and is convenient when using file download tools provided by VeriFone such as VeriCentre Download Management Module (DMM), VeriCentre, and the direct download utility, DDL.EXE. In command-line mode, you can sign a batch of files in a single operation.
- **Graphical interface mode** (Windows NT or Windows 95): Use the FileSign dialog box (Figure 20) to select the file to sign and assign a name and destination location for the generated signature file on the host computer. When you run the FILESIGN.EXE tool under Windows, you can sign only one file at a time.

  You can also specify to store the target file in the target file group's RAM (default location) or in the flash file system. If required, you can navigate through the file system on your PC to select the signer certificate file (*.crt) and signer private key file (*.key) to use as inputs to the file signing process.

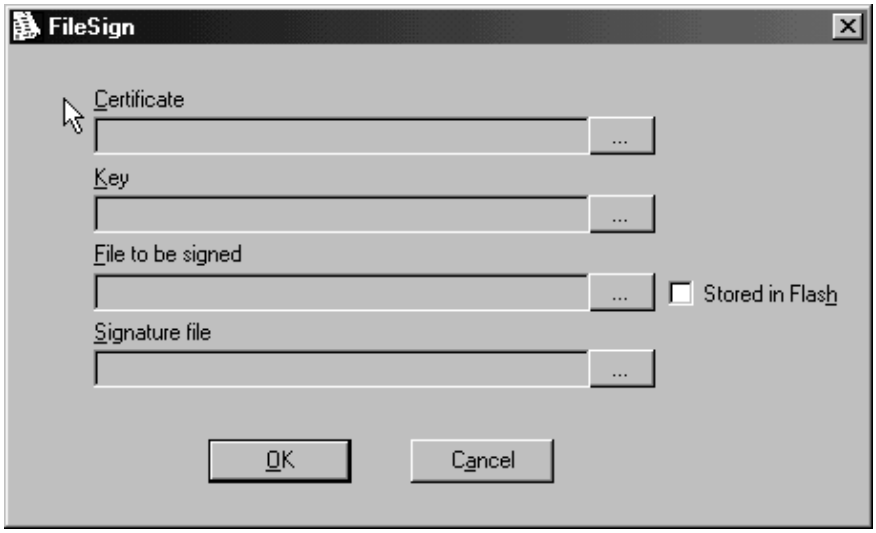


Figure 20 FileSign Dialog Box for FILESIGN.EXE Under Windows

NOTE

If the entry of a signer password is a required input, a secondary dialog box displays to enter and confirm the password. Please also note that a signer password is required for a deployment terminal, but not for a development terminal.

Command-Line Entries for FILESIGN.EXE

Table 18 lists and describes the *switches* that make up the command-line mode syntax for FILESIGN.EXE.

Table 18 Command-Line Mode Switches for FILESIGN.EXE

Switch	Description	Requirements
-C, -c	Signer certificate file name (*.crt).	Required input for development terminals and deployment terminals. For development terminals, you can use the default signer certificate, K2SIGN.CRT. For deployment terminals, you must use the signer certificate issued by the VeriFone CA.
-K, -k	Signer private key filename (*.key).	Required input for development terminals and deployment terminals. For development terminals, you can use the default signer private key, K2SIGN.KEY. For deployment terminals, you must use the signer private key provided by the VeriFone CA.
-P, -p	Signer password for decrypting the signer private key.	Required input only for deployment terminals. The VeriFone CA issues and securely conveys this password to an authorized signer.
-F, -f	Name of the application file to sign (*.out, *.lib, or other file type).	Required for development terminals and for deployment terminals.
-S, -s	Name of the signature file (*.p7s) for FILESIGN.EXE to generate for the target application file.	Required for development terminals and for deployment terminals.
-L, -l	Specifies to store the target application file to sign and authenticate in the flash (drive F:) file system. If you do not use this switch to specify flash as the target file destination, it is stored by default in the RAM file system (drive I:).	Optional entry. This switch assigns an F: prefix to the name of the *.out or *.lib file to download, and also stores this information in the signature file as part of the special filetype attribute. **Note:** **NOTE:** Signature files must be downloaded into the target file group's RAM. If the target file is authenticated, the corresponding *.p7s file is moved to the same memory area as the target file it authenticates. For example, if the target file is stored in flash (F:), its *.p7s file is moved into the flash file system. If, however, you set the *FA variable in the file group's CONFIG.SYS file to 0, all signature files are deleted from RAM when file authentication is complete.

Command-Line Mode Syntax Example

In the FILESIGN.EXE command-line entry example below, please note that the syntax used applies to an Omni 37xx development terminal with the factory set of certificates, and not to a deployment terminal. There are two differences:

- The default signer certificate and default signer key file names that are provided by VeriFone as part of the Omni 37xx SDK are entered on the command line instead of customer-specific customer signer certificate and customer signer private key file names.
- The switch for signer password (`-P password`) is not used, because a customer signer password is only required to sign and authenticate files for Omni 37xx deployment terminals being prepared for deployment.

Please note also how the command-line mode switches described in Table 18 are used in this example:

```
filesign -L -f file.out -s file.p7s -c k2sign.crt -k k2sign.key
```

- The `-L` switch indicates to store the application file in the flash file system instead of the target group's (default) RAM file system. (The target group for the download must be selected from system mode when the download is performed.)
- The `-f` switch indicates that the application file "`file.out`" must be signed by the FILESIGN.EXE tool.

  Executable files, such as *.out and *.lib files, must always be signed if they are to run on the terminal following a download. Depending on the application's logical security requirements, other types of files, such as data files and font files, may also need to be signed and are authenticated on download.
- The `-s` switch is followed by the name of the signature file to generate, `file.p7s`.
- The `-c` switch is followed by the name of the default signer certificate to use for file authentication with the development terminal, `k2sign.crt`.
- The `-k` switch is followed by the name of the default signer private key file, `k2sign.key`. A signer private key is a required input to the file signing process for development terminals and for deployment terminals.

FILESIGN.EXE Graphical Interface Mode

When you execute FILESIGN.EXE in the Windows environment, the FileSign dialog box displays (see Figure 20).

The FileSign dialog box has four entry fields, each of which is followed by a "Next" [**...**] selection button, as well as one check box, and the OK and Cancel buttons:

- Press `ALT-C` or click on the [**...**] button to the right of the "Certificate" field to locate and select the certificate file (*.crt) you want to use to sign the file.
- Press `ALT-K` or click on the [**...**] button to the right of the "Key" field to locate and select the signer private key file (*.key).
- Press `ALT-F` or click on the [**...**] button to the right of the "File to be signed" field to locate and select the application file (*.out, *.lib, or other) to sign. If necessary, you can also modify the filename.

If you want to store the file in flash memory on download to the terminal, check the “Stored in FLASH” checkbox. This adds the “F:” prefix to the target file name.

- Press ALT-S or click on the [**...**] button to the right of the “Signature file” field to enter a filename for the signature file to be generated. The filename extension must always be *.p7s. You can also choose another directory to store the generated signature file.
- When all entries are complete, press ALT-O or click the OK button to execute FILESIGN.EXE and generate the signature file. Or, press ALT_A or click Cancel to exit the FILESIGN.EXE utility.

When the necessary signature files are generated to authenticate the application or applications on the Omni 37xx terminal, you are ready to perform the application download procedure.

For more information about file authentication within the context of specific download procedures, please refer to Chapter 6.

CHAPTER 6

Performing Downloads

This chapter contains information and procedures to allow you to perform the various types of data transfers required to:

- Develop applications for the Omni 37xx terminal.
- Prepare Omni 37xx terminals for deployment.
- Maintain Omni 37xx terminal installations in the field.
- Transfer data to/from terminals.

In this chapter, information pertaining to file authentication is only discussed in the context of procedures while performing file downloads. See Chapter 5 for further file authentication discussion.

The Omni 37xx terminal contains ports that allow connection to a network, telephone line, or other terminals (for back-to-back downloads). See Download Methods.

Downloads and Uploads

In downloads, data transfers from a sending system to a receiving system. The term *download* also refers to a terminal receiving data. The term *upload* describes the process of a terminal sending data.

Use any of the following three operations to program, deploy, transfer data files from, and support Omni 37xx terminals:

- *Host* computer downloads: Applications, operating systems or OS updates, and associated files transfer from a host PC to a Omni 37xx terminal
- *Back-to-back* downloads: Applications and associated files transfer from one Omni 37xx terminal to another Omni 37xx terminal

Download Methods

The following four methods are available for file and data downloads through the Omni 37xx download and upload procedures:

- **Direct downloads:** Files and/or data transfer directly from the sending system (a host computer) to the receiving system (an Omni 37xx terminal). A special cable (VPN 05651-xx) connects the RS232 serial ports of the two systems.
- **Downloads by telephone:** Files and data transfer over a telephone line from the sending system (a host computer) to the receiving system (an Omni 37xx terminal). The modem of the sending host computer, and the internal modem of the sending receiving terminal are connected by a telephone line connection. Data transfers into the Omni 37xx terminal through the communication port contacts.

- **Back-to-back downloads:** Files and data transfer from a sending Omni 37xx terminal to a receiving Omni 37xx terminal. A special cable (VPN 05651-xx) connects the RS232 serial ports of the two terminals.

Download Tools

Three software tools are available from VeriFone for performing downloads: **VeriCentre Download Management Module (DMM)**, VeriCentre, and **DDL.EXE (Direct Download Utility)**.

NOTE

Because of the large size of some download files, VeriFone recommends only using download tools provided by VeriFone; these tools provide error checking mechanisms.

These tools perform direct downloads and downloads by telephone from a host computer to an Omni 37xx terminal:

- **VeriCentre DMM:** Multi-user environment for software downloads. DMM supports Windows NT clients and has a sophisticated database to manage up to 100,000 terminals. The Omni 37xx operating system supports file decompression for archives created using DMM.
- VeriCentre**:** PC-based software tool to manage applications and data for VeriFone. In addition to being a database and communications management tool, VeriCentre automates application downloads and updates to terminal records.
- **DDL.EXE:** Download files and data from a development system or other host computer directly to an Omni 37xx terminal over a serial cable connection. DDL.EXE is a 32-bit, Windows 95 program included in the VDTK (Verix Developer's Toolkit).

NOTE

No special software tool or utility is required to perform back-to-back application downloads. Only a serial cable connected between two terminals is required. This data transfer procedure, invoked from within system mode, is handled by the OS software and firmware of the sending and receiving Omni 37xx terminals.

Download Content

In general, you can download files *and* data to an Omni 37xx terminal. The types of files and data can be grouped into the following functional categories:

- **Operating system files:** A set of related programs and data files provided by VeriFone to control the terminal's basic processes and functions. Files that belong to the OS are stored in a reserved area of the terminal memory.

  A complete OS is downloaded to each Omni 37xx terminal during the manufacture. If necessary, download newer versions during application development, when preparing for deployment, or to terminals in the field.

- **Applications and related files:** An application is a computer program consisting of one or more executables, including compiled and linked object files (*.out), and one or more function libraries (*.lib). Most applications also include font files (*.vft, *.fon), data files (*.dat), and other related file types.

Omni 37xx applications can be developed by VeriFone, customers, or third parties on customer request. One or more applications must be downloaded to the Omni 37xx terminal before it can be deployed at a customer site and used to process transactions.

- **Files related to file authentication:** The logical component of the VeriShield security architecture in the Omni 37xx terminal is *file authentication*. For an executable to run on an Omni 37xx terminal, it must be authenticated by the VeriShield file authentication module.

NOTE

For a details on file authentication, see Chapter 5.

Two special types of files are required for the file authentication process: digital certificates (*.crt) and signature files (*.p7s). These file types must be downloaded to the terminal together with the application files to authenticate.

- **Terminal configuration settings:** Files or records that contain various types of data can also be downloaded to an Omni 37xx terminal, including CONFIG.SYS variables, passwords for accessing protected system mode functions, the current date and time, the modem country code setting, and so on (refer to Chapter 4).

Full and Partial Downloads

When preparing to initiate a download procedure, you must choose either a *full* or *partial* download and the COM 1 port, through the system mode menu options (refer to Chapter 4). Depending on the type of files you are downloading and the download method you are using, there are some restrictions on if a full or partial download is permitted.

The various types of full and partial download procedures are listed and described in Table 19.

Table 19 Types of Full and Partial Downloads

Download Type	Description and Effects	Download Methods Supported
Full application download	An entire application, including all executables and data files, transfers from one system to another in a single operation. Files related to the file authentication process and terminal configuration settings can be included in a full application download. During this process RAM is cleared. Following a full application download, the terminal restarts and the file authentication module is invoked. If application files are authenticated, the application executes.	• Direct downloads • Telephone downloads • Back-to-back downloads
Partial application download	A subset of application executables, font files, and/or data files transfer from one system to another to modify or update an existing application. Files related to file authentication and terminal configuration settings can be included in a partial application download. During this process, RAM is *not* cleared. Following a partial application download, the terminal does not restart and returns control to system mode or the issuing application. The file authentication module is not invoked, nor is the application allowed to execute, until the terminal is manually restarted from within system mode.	• Direct downloads • Telephone downloads **Note:** Partial back-to-back downloads are *not* supported.

Table 19 Types of Full and Partial Downloads

Download Type	Description and Effects	Download Methods Supported
Full operating system download	An *entire* OS version transfers from a host PC to the Omni 37xx terminal. Files related to file authentication and terminal configuration settings can be included in a full OS download. During this process, RAM is cleared. Following a full OS download, the terminal restarts and the file authentication module is invoked. If the OS files are authenticated, the new OS updates (replaces) the existing OS. Application files stored in the memory area where the OS downloads (Group 1) are erased.	• Direct downloads • Telephone downloads **Note:** Full back-to-back OS downloads are *not* supported
Partial operating system download	Either an *entire* or a *partial* OS version transfers from a host PC to the Omni 37xx terminal. Files related to file authentication and terminal configuration settings can be included in a partial OS download. Following a partial OS download, the terminal does not restart and returns control to system mode or the issuing application. The file authentication module is not invoked, and the new OS is not processed until you manually restart the terminal from within system mode. If the new OS is authenticated, it then updates (replaces) the existing OS. Application files stored in the memory area the OS downloaded into (Group 1) are retained.	• Direct downloads • Telephone downloads **Note:** Partial back-to-back operating system downloads are *not* supported.

Here are a few more points on the topic of full and partial downloads:

- The most common download procedure is a full (complete) application download.
- Partial application downloads are useful when developing and testing new applications, but are seldom performed by those who deploy terminals or in the field.
- Full OS downloads are usually performed by VeriFone at the factory and, on occasion, by those who deploy terminals or in the field to upgrade older terminals to a newer OS version.
- Partial OS downloads are performed mainly by VeriFone for development purposes and are rarely performed in the field.
- Partial downloads are routinely performed by many applications. This procedure, which can be automated by an application running on a remote host computer, permits the host application to update data files and terminal

configuration settings in an Omni 37xx terminal and then return control to the main application.

- Full downloads restart the terminal; partial downloads return control to system mode or the issuing application. OS and application downloads can be combined. The file authentication module is not invoked until the terminal is restarted following the download procedure.

Omni 37xx Download Differences

To help you plan download tasks and explain how the download procedures for Omni 37xx terminals may differ from those you may be accustomed to using for other POS terminals, some information on the following related topics is included in this chapter:

- Support for multiple applications
- Use of RAM and flash memory
- Redirection of files during application downloads
- File authentication requirements

Support for Multiple Applications

The Omni 37xx terminal architecture supports multiple applications. This means that more than one application can reside in terminal memory, and that more than one application can run (execute) on the terminal.

The application memory of the Omni 37xx terminal uses a system of file groups to store and manage multiple applications, as well as operating system files, in such a way that the data integrity of each application is ensured and that applications do not interfere with each another (see File Groups).

How the File System Supports Multiple Applications

The application memory partition of the Omni 37xx terminal is divided into 15 logically-defined sub-partitions called file groups or GIDs These groups are called Group 1, Group 2, and so on through GID15.

Another partition of the terminal memory area, called Group 0, is reserved for the operating system and is logically separated from the application memory area. So, including Group 0, there is a total of 16 file groups.

An application must be downloaded into a specific file group, along with any related files. You select the target file group for the download using system mode menu options and by entering a file group password.

Usually, one application is stored in one file group. An application can, however, consist of more than one executable program file, and any number of executables (*.out or *.lib) can be stored in a given group. In most implementations, there is a main application, one or more related programs or secondary applications, and one or more libraries.

The main application must always be stored in the Group 1 sub-partition. Related programs or secondary applications can be stored in GIDs 2–14. GID15 is available to all other groups.

The Main Application is Always Stored in GID1

The main application stored in GID1 is the controlling application for the terminal. Any function call that invokes a related program or a secondary application stored in GIDs 2–14 must be initiated by the GID1 application.

An application stored in a file group other than GID1 is limited in that it can only access executables and files stored in its own file group and in GID15.

Physical and Logical Access to File Groups

The Omni 37xx operating system controls *physical* access to GIDs 1–15 using password-protected system mode functions.

To download data into a specific file group, you must first enter system mode and choose the target group by making the appropriate menu selections. Then, you must enter the correct password for that file group.

Each file group has its own CONFIG.SYS file. The CONFIG.SYS settings of the target group you select are always used as the system parameters for the download operation you are performing.

The system of file groups also imposes some *logical* restrictions on which files can download into which file groups:

- If GID1 is selected as the target group in system mode, you can download files into GID1 and redirect files into any of the other file groups, as required, in the same download operation.
- If another file group is selected as the target file group, you can download files only into that group and redirect files only to GID15. For example, if you select GID5 as the target group for the download, files can only download into GID5 and be redirected to GID15.

Use of RAM and Flash Memory

The Omni 37xx application memory partition has two separate file systems:

- RAM (battery-backed volatile memory, also called SRAM), drive name I:
- Flash (non-volatile memory), drive name F:

The fact that there are two different file systems has the following important implications for data transfer procedures:

- Depending on the requirements of a specific application, some files must download into RAM and others into flash.
- There are also rules that restrict which types of files you can download and store in which file system (RAM or flash).

With application files, the application designer or programmer usually decides which file types to download into which file system. Other file types, such as operating system files, digital certificates, and signature files, *must* download into RAM.

In a typical download procedure, all files are loaded into the RAM file system of the target group selected in system mode. Specific files included in the download package must be redirected, as necessary, to the flash file system of the target group or to the RAM or flash file system of another file group.

To redirect files during a download procedure, see the following sections.

Defragment Flash For Application Downloads

Before you perform an application download, you may need to defragment terminal flash memory. For information on performing this system mode operation, see System Mode Menu 2.

To ensure the best result when performing back-to-back downloads, you may need to defragment the flash memory of both the sending *and* receiving terminals. A system mode procedure is also available for clearing the RAM or flash memory, either entirely or for a specific file group, to prepare an Omni 37xx for a *clean* download.

NOTE

The flash defragment operation is not necessary for an Omni 37xx terminal just out of the box. In this case, the terminal flash file system is still in its factory-new condition.

Redirection of Files During Application Downloads

You can download application files into RAM or flash memory. By default, files that you download to a specific file group are stored in the RAM of that group. To store a file in flash of that file group, you must provide instructions to redirect the file to flash as part of the procedure.

There are two methods you can use to redirect files during an application download, depending on the download tool you are using:

- If you are using Download Manager or VeriCentre, you must manually create and include special zero-length files called SETDRIVE.x and SETGROUP.n on the download computer, and add these files to the batch download list to direct files to a specific file system (drive) or file group.
- If you are using DDL.EXE to perform direct downloads, you can use a special command-line option that automatically redirects files to the drive and file group you specify.

Both of these methods are described in the following sections.

Manually Redirecting Files to Flash Memory

To manually redirect files to flash memory for Download Manager or VeriCentre application downloads, you must create one or more files on the download computer with the special file name, SETDRIVE.x, where, *x* is the name of the drive (memory area) to download files to:

- Drive name I: is RAM: This is the system mode default for downloads.
- Drive name F: is flash.

To create a zero-length SETDRIVE file on the download computer, use the DOS command, REM, as in the following example:

```
REM >SETDRIVE.F
```

To redirect a file from RAM of the target group to flash of the same file group, insert the zero-length SETDRIVE.F file into the batch of application files to download. All files that follow the SETDRIVE.F file in the download list automatically load into flash memory (F:) of the target group.

If you do not insert a SETDRIVE.F special file in the download list, all files download by default into the RAM (drive I:) of the target file group. You can also insert a zero-length file with the name SETDRIVE.I into the download list at any point to indicate that the following files download into RAM.

For example, the following batch download list loads the executable code file FOO.OUT into the RAM of the selected file group (default Group 1). Because the signature file, FOO.P7S is included, FOO.OUT is also authenticated when the terminal restarts after the download.

The *GO variable in this example indicates that the FOO.OUT application executes on restart, after successful authentication. The two data files that follow the zero-length SETDRIVE.F file, FOO.DAT and FOO.VFT, are redirected into flash of GID1. Because it follows the inserted zero-length SETDRIVE.I file, GOO.DAT downloads into Group 1 RAM.

```
FOO.OUT
FOO.P7S
*GO=FOO.OUT
SETDRIVE.F
FOO.DAT
FOO.VFT
SETDRIVE.I
GOO.DAT
```

You can also insert zero-length SETGROUP.n files into a batch download list to redirect files from the target file group to other file groups. Together, the zero-length SETDRIVE.x and SETGROUP.n files allow you flexibility to store files as required in RAM or flash file systems and in specific file groups in a single batch download operation.

NOTE

You can only use zero-length SETDRIVE.x files for *batch application downloads*, either direct or telephone, and only using the Download Manager or VeriCentre download tools (and not DDL.EXE).

You cannot use this special file convention for operating system downloads or for back-to-back application downloads.

Redirecting Files to Other File Groups

GID1 is the default system mode setting for performing downloads. Using the system mode menu options, you can select another file group (GID 2–15) as the target group for the application download. If you select another group, files download directly into the RAM of that file group.

To redirect files from the selected target file group to another file group as part of the download operation, insert a zero-length SETGROUP.n file in the batch download list (the same as SETDRIVE.x). The syntax of this convention is SETGROUP.n, where *n* = 1–15, for GIDs 1–15.

To create a zero-length SETGROUP file on the download computer, use the DOS command REM as in the following example:

```
REM >SETGROUP.2
```

If you do not insert SETGROUP.n special files into the download list, all files download into the target group selected in system mode. If no number is added to the SETGROUP filename, SETGROUP.1 (GID1) is assumed.

Restrictions on File Redirection

The Omni 37xx file system restricts how you can redirect files to other file groups. Here are the important points to remember:

- The main application must always be downloaded into GID1.
- Because of the way file groups are managed in the Omni 37xx file system, only two schemes are available for redirecting files during a batch application download:
  - If, using system mode menu options, you select Group 1 (default) as the target group for the download, files can be redirected to any other file group, including GID15.
  - If, using system mode menu options, you select a file group other than Group 1 (GIDs 2–14) as the target group for the download, files can be redirected only into the selected file group or into GID15.

In the following example, GID1 is selected as the target group for the download. The download list loads FOO.OUT into Group 1 RAM, GOO.OUT into GID2, and the shared library, COMN.LIB, into GID15. When the terminal restarts after the download, the file authentication module is invoked for all three files, based on the certificate data that authorizes them to be stored in their respective file groups.

If FOO.OUT is authenticated, the GID1 application, FOO.OUT, executes, as specified by the *GO variable, when the terminal restarts following successful file authentication. The function library stored in GID15 can be shared by both applications, as both Group 1 and Group 2 applications can access Group 15:

```
FOO.OUT
FOO.P7S
*GO=FOO.OUT
```

```
SETGROUP.2
GOO.OUT
GOO.P7S
SETGROUP.15
COMN.LIB
COMN.P7S
```

NOTE

You can only use zero-length SETGROUP.x files for *batch application downloads*, either direct or telephone, and only using the Download Manager or VeriCentre download tools (not DDL.EXE). You cannot use this special file convention for operating system downloads or back-to-back application downloads.

Using DDL.EXE to Automatically Redirect Files

The version of DDL.EXE included in the Omni 37xx SDK allows you to change the default drive and file group for a direct download by preceding the filename(s) on the DDL command line with a special filename. The syntax is as follows:

`SETDRIVE.<drive letter>`

where, `drive letter` is `I:` (RAM, default) or `F:` (flash), and/or

`SETGROUP.<group number>`

where, `group number` is `1–15`.

For example, the following command-line entry:

```
DDL SETDRIVE.F cardco.lib SETDRIVE.I SETGROUP.15 card.dat
```

downloads the executable file `cardco.lib` into the flash of the selected target group and the data file `card.dat` into Group 15 RAM. (Because drive or group settings apply to all files that follow in the list, it is necessary to use SETDRIVE.x to reset the drive from `F:` back to `I:`.)

If you are using this DDL.EXE method, zero-length SETDRIVE.x and SETGROUP.n files do not need to exist as files on the download computer.

File Redirection in Operating System Downloads

When performing an operating system download, you *must* download the OS files into Group 1 RAM and not into flash memory or into another file group.

OS files download into Group 1 RAM because is not possible to download these files directly into Group 0. OS files are redirected to Group 0 depending on if you perform a full or partial download (see Table 19):

- For full OS downloads, the redirection of OS files into Group 0 is performed automatically, after the terminal restart, as part of the download procedure.
- For partial OS downloads, OS files are redirected from the RAM of Group 1 into Group 0 on manual terminal restart by selecting the appropriate system mode menu option.

A downloaded OS is processed and authenticated while stored in Group 1 RAM. As the files are authenticated under the authority of the certificates and signature files included in the OS download package, they move automatically into Group 0. This process, which usually takes a few minutes, is completely transparent during the download procedure.

File Redirection in Back-to-Back Application Downloads

In a back-to-back application download, *all* application files stored on the sending terminal — in both file systems and in all file groups — transfer to the receiving terminal in a single operation.

For this type of download, you *must* select Group 1 as the target group on the sending *and* receiving terminal. When you initiate the download on the receiving terminal, all application files, as well as all special files required for file authentication and terminal configuration settings on the sending terminal, download to the receiving terminal.

In this type of data transfer operation, some file redirection does occur automatically as a result of the file authentication procedure that occurs on the receiving terminal. This redirection process is transparent during the download.

Briefly, all files initially download into RAM, and are then redirected based on the directory and subdirectory names of the sending terminal's file system. Signature files must always be authenticated in RAM. If the target file the signature file authenticates is stored in flash, the signature file is moved to flash only after the target file is successfully authenticated.

To successfully perform a back-to-back download, all signature files that are required to authenticate application executables must reside in the memory of the sending terminal. If the *FA variable is present in the Group 1 CONFIG.SYS file of the sending terminal, it must be set to 1 to retain all previously downloaded signature files.

If a signature file is missing on the sending terminal, the target application file that it authenticates is not authenticated on the receiving terminal and, if the target file is an executable, it is not allowed to run on the receiving terminal.

File Authentication Requirements

Chapter 5 provided a general introduction to the file authentication process. Now we become more task-oriented and see how the file authentication process affects how to perform the various download procedures.

Required Certificates and Signature Files

Here are some important points to remember about how certificates and signature files relate to application download procedures:

- Before an executable file can be downloaded to and be allowed to run on an Omni 37xx terminal, the file must be digitally signed on the download computer using the file signing tool, FILESIGN.EXE. The result of this procedure is a signature file recognized by its *.p7s file name extension.

- A signature file must be downloaded together with each executable that makes up an application. An executable can be a compiled and linked object file (*.out) or a shared function library (*.lib).

  In most cases, an application consists of multiple executables and requires a number of corresponding signature files.
- In a typical batch application download, all files, including executables, signature files, and any required certificates, download together in the same operation.
- After the download is complete and the terminal restarts, the file authentication module is invoked if a new signature file (or certificate) is detected. If the application (executable) is authenticated, it is allowed to run on the terminal. Otherwise, it does not execute.
- If one executable file is required by an application that consists of multiple executables fails to authenticate, the main application may crash when it attempts to access the non-authenticated executable.
- Application files other than executables (for example, font and data files) may also require logical security under file authentication. In these cases, each protected non-executable file also requires a corresponding signature file.
- Digital certificates (*.crt) and signature files (*.p7s) required to authenticate both application files and operating system files must always be downloaded into RAM of the target file group.
- Certificate files are deleted from application memory after they are authenticated. If a certificate is not authenticated, it is retained in the terminal memory.
- If the *FA variable in the CONFIG.SYS file of the target group is set to 1, signature files are redirected to the same location where the application file it authenticates is stored. If *FA is 0, signature files are deleted from RAM when the file authentication process is complete.

The File Authentication Process During an Application Download

In the following example of a typical file authentication process, it is assumed that we:

- are downloading an application to prepare an Omni 37xx deployment terminal for deployment. That is, a sponsor certificate and a signer certificate download in batch mode to GID1 RAM of the receiving terminal, together with the application to authenticate.
- generated a signature file for each executable that comprises the application on the download computer using FILESIGN.EXE, with the signer certificate, signer private key, and signer password as required inputs. These signature files are also downloaded to the receiving terminal.

In a typical batch application download, file authentication proceeds as follows:

1. All certificate files (*.crt), signature files (*.p7s), and application files (*.out, *.lib, *.fon, *.vft, *.dat, and so on) download to the Omni 37xx deployment terminal in batch mode.
2. When the terminal restarts after the download, the file authentication module searches the RAM-based file system for the following two file types:
   - Authenticated certificate files (*.crt) to add to the permanent certificate tree
   - Signature files (*.p7s) that authenticate corresponding target application files

   Certificate files and signature files can download into the RAM of any file group. For this reason, the file authentication module searches through the entire file system (all file groups) for new files with these filename extensions each time the terminal restarts.
3. The file authentication module builds a list of all newly detected certificates and signature files. If no new certificates or signature files are located, the module just returns. If one or more new files of this kind are detected, the file authentication module starts processing them based on the list.
4. Certificates are always processed first (before signature files). The processing routine is called one time for each certificate in the list. If a certificate is authentic, it is noted, and the next certificate processed. This process continues in random order until all certificates are authenticated.

   When a certificate file in the processing list is authenticated, the “Authenticated” message displays below the corresponding filename. If it fails to be authenticated, the “Failed” message displays for five seconds and the terminal beeps three times (see Figure 21). The routine then resumes processing and continues until all certificates are successfully processed.

   The processing routine gives you both visible and audible indications if a specific certificate successfully authenticates. The file authentication module does not halt the process if a certificate fails to authenticate, but continues to the next step: authenticating signature files.

   If one or more certificates fail to authenticate, the ensuing file authentication process based on signature files probably also fails, with the result that an application is not authenticated and is not allowed to execute on the terminal.

   When a certificate file is authenticated, the data it contains is added to the certificate tree and the certificate file is deleted from the RAM. When all required certificates are authenticated and stored in the certificate tree, the file authentication process for signature files can proceed.

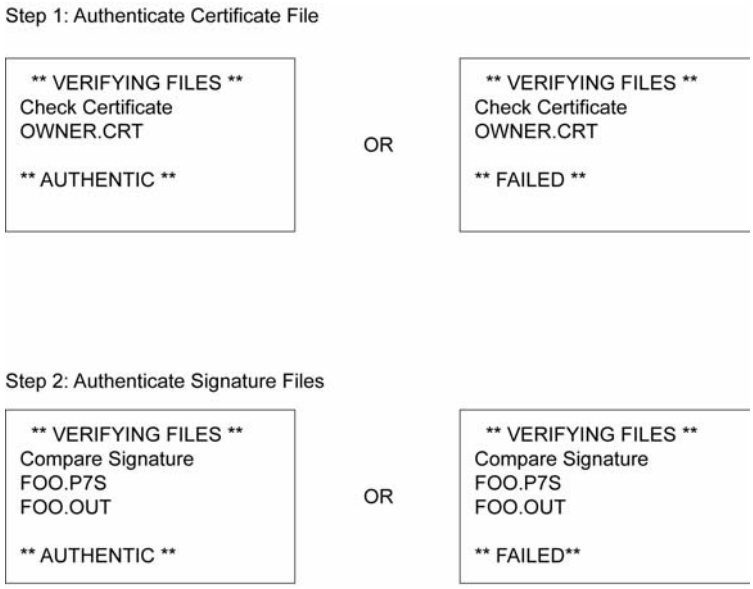


Figure 21 Display Prompts During the File Authentication Process

5 Signature files are processed next (after certificate files). The file authentication module calls the signature checking routine one time for each new signature file it detects. Each *.p7s file is checked as it is detected; a list is not built and multiple processing passes are not required.

- If a signature file is authenticated, the "AUTHENTIC" message displays and the target file's ATTR_NOT_AUTH bit is set to 1.
- If the authentication process fails, the "FAILED" message displays for five seconds and the terminal beeps three times (see Figure 21). The routine then continues processing the next signature file until all newly detected signature files are checked.
- If a signature file fails to authenticate and its target file is an executable code file, such as *.out or *.lib, the executable is not allowed to run on the terminal on terminal restart.

For data files, font files, and any other files that require authentication to meet the application's design specification, the application must ensure that these files successfully authenticate.

While a signature file is being processed, it remains stored in the RAM file system of the target file group. The target application file may be redirected immediately on download to RAM or flash.

When the signature file successfully authenticates its target file, it is automatically moved to same the file system and file group as the target file it authenticates (that is, if *FA = 1).

The processing routine gives you visible and audible indications of if a specific signature file successfully authenticates. The file authentication module does

not halt the process if a signature file fails to authenticate, but continues to the next step: storing the downloaded files in their final locations in the terminal file system.

6 Certificate files and signature files are retained in the RAM file system until the file authentication process is complete. These special files are then either deleted or automatically redirected to another file system or file group, as previously described.

When an application file is authenticated, the operating system sets the file's read-only attribute to protect it from being modified while stored in terminal memory. This is also true for a signature file retained in terminal memory. When a signature file is assigned the read-only attribute, it is no longer detected as a new signature file by the file authentication module on terminal restart.

7 When all certificates and signature files are processed and special files deleted or redirected as required, the terminal restarts and the *GO application executes.

File Group Permissions

Now, consider how file authentication controls *who* (which business entity) can store application files in which file groups in the Omni 37xx file system.

By inserting zero-length SETDRIVE.x and SETGROUP.n files into a download list, you can specify which drive (*x* = I: RAM or F: flash) and which group (*n* = 1–15) to store an application file. In addition to this file redirection protocol, the file authentication module controls which files are allowed, under the authority of the signer certificate used to sign them, to be stored in which file groups in the Omni 37xx file system.

For example, if the terminal owner specifies that a *loyalty* application in be stored GID2, the information is encoded in the sponsor and signer certificates issued by the VeriFone CA for that terminal.

Chapter 5 discussed how signer certificates are required inputs to FILESIGN.EXE when preparing a deployment terminal. Each signature file generated under that signer certificate contains a logical link that allows the application to authenticate and run on the terminal *only* if the signature files and corresponding target files are downloaded into the target GID.

Although you *can* store files in any file group simply by selecting the target group in system mode, the files you download are not authenticated for the target group you selected unless they are properly signed under the authority of the sponsor and signer certificates issued for that terminal.

Download an Operating System Update Provided by VeriFone

Because the operating system software for the Omni 37xx is developed and controlled by VeriFone for its customers, VeriFone provides the necessary certificates and signature files to ensure the authenticity and integrity of the operating system update as part of the download package.

NOTE

Operating system files can only be transferred to an Omni 37xx terminal using a PC-to-terminal download procedure, either direct or by telephone. OS files cannot be downloaded to an Omni 37xx terminal in a back-to-back operation.

The file authentication procedure for OS downloads is much the same as application downloads, with the following exceptions:

- VeriFone provides all files required for the OS download, including:
  - The operating system files (such as Q.out, 1.out, and 2.out)
  - An encrypted list of the new files, called VFI.PED
  - A signature file generated by the VeriFone CA under the authority of a higher-level OS *partition sponsor certificate*, called VFI.P7S

    The file authentication logic on the receiving terminal uses this signature file to confirm the origin and authenticity of the encrypted list of files, VFI.PED.
- You *must* download the entire OS package into Group 1 RAM. If you select a target group other than Group 1, the operation fails.
- Before you initiate an OS download, either full or partial, ensure enough memory space is available in Group 1 RAM to temporarily store the OS files and that any application files can also be stored in Group 1.
- If you have selected a *full* OS download in system mode, the terminal restarts automatically and the new OS is processed and replaces the existing OS. In this download operation, all application files stored in Group 1 are automatically erased.
- If you select a *partial* OS download, the operating system returns control to system mode after the download completes. To process the new OS, you must *manually* restart the terminal by selecting the appropriate system mode menu option. In a partial OS download operation, application files stored in Group 1 are not erased.
- When you initiate the OS download, the OS file authentication progress displays on the screen as new certificates are authenticated and added to the terminal's certificate tree, and as signature files for corresponding OS files are detected and authenticated, as shown in Table 21.
- While the new OS is being processed, there is no visible indication on the terminal display of progress. When the new OS is processed (this usually

takes a few minutes), the terminal restarts automatically and the OS download procedure is complete.

CAUTION

If the power supply to the receiving terminal is accidentally cycled during an operating system download procedure, the terminal may permanently lock up. In that case, return the terminal to VeriFone for service.

File Authentication for Back-to-Back Application Downloads

When performing a back-to-back application download between two Omni 37xx terminals, the file authentication process on the receiving terminal is similar to an application download from a host computer to a standalone Omni 37xx terminal. There are, however, some important differences to take into account:

- Only a *full* application download is supported for back-to-back data transfers. You cannot perform partial back-to-back application downloads.
- Before you can initiate the back-to-back download, you must enter system mode in *both terminals*, select Group 1 as the target group for both terminals, and enter all required passwords.
- All signature files required to authenticate the download application(s) must reside in memory of the sending terminal. They *must not be deleted* through the *FA variable being cleared to 0 on previous downloads.
- Any sponsor and signer certificates downloaded to and authenticated on the sending terminal are stored in the certificate tree of that terminal. When you perform a back-to-back download, certificate files are reconstructed from the data present in the sending unit's certificate tree.
- All certificates transfer to Group 1 RAM on the receiving terminal, except for the highest-level *platform root certificate*, which can never be transferred to another terminal.
- When certificates are detected by the file authentication module of the receiving terminal, they are processed exactly the same as in a direct download: All certificates are checked one by one and, on authentication, are added to the certificate tree of the receiving terminal. Then, all signature files are checked.
- Downloaded certificates (receiving terminal) must synchronize with the certificate data present in the certificate tree.
  Here, synchronized means that the certificate tree of the receiving terminal can be no more than one revision out-of-sync with the certificate tree on the sending terminal or the files on the receiving terminal do not successfully authenticate. In this case, the term *revision* refers to any generic change to the current sponsor and signer certificates stored in the certificate tree of a deployment terminal.
- When the back-to-back download completes and all certificates and signature files authenticate, the receiving terminal restarts. If the name of the *GO application is specified in the Group 1 CONFIG.SYS file of the receiving

terminal, the application executes and the application prompt or logo displays on the terminal.

Timing Considerations Due to the Authentication Process

The file authentication process takes some time. The total amount of time required depends on a number of factors:

- the number and size of application files
- the number of certificates and signature files
- whether the file compression feature of Download Manager is being used to perform the download

Here are a few additional considerations that may affect the total elapsed time required to complete the download operation:

- Because additional processing steps are required, an operating system download takes longer to complete than an application download (several minutes as opposed to a few seconds).
- The download order of a batch of certificate files may affect total processing time. Digital certificates are validated in a looping process where the validation process cycles as many times as necessary to establish the proper relationship and position of a given certificate in the certificate tree that exists in the terminal.

  To optimize the authentication process, you can download certificates in a higher-level-certificates-first order. This way, they process faster than a random order download.

Optimize Available Memory Space for Successful Downloads

One certificate file or signature file requires approximately 400 bytes of memory space. The application designer must account for the extra memory required to download and store these special files.

When planning your download procedure, carefully consider the total amount of memory space required to store certificates and signature files *and* the application files. In some cases, a considerable number of 400-byte signature files reside in terminal memory at any given time. Here are some general guidelines to follow:

- Know the size of available memory (RAM and flash) of the receiving terminal; in back-to-back downloads, memory on both the sending and receiving terminal.
- Know in advance how application files are redirected to RAM or flash and to file groups other than the target group.
- Defragment flash memory before performing a download to optimize the available space in the flash file system.

- Before you perform a download, use system mode menu selections to clear the entire RAM and/or flash or the RAM or flash of a specific file group, as necessary to ensure proper use of available memory in the target group.

Support for File Compression

For information regarding file compression, refer to refer to the *Verix Operating System Programmer's Manual* (VPN 19733).

Effect of Downloads on Existing Files and Data

When you download application files and data to an Omni 37xx terminal, an important consideration is the effect of download procedure on existing application files, files used in the file authentication process, and terminal configuration settings stored in CONFIG.SYS files in the receiving terminal. Here are some important points to remember:

- If a file already exists in the target file group, the existing file is replaced with the new file of the same name. (Files in separate file groups can have identical names.)
- Always download executable files (and any other files to logically protect under VeriShield file authentication) together with the certificates and signature files required to authenticate them.
- In full or partial application downloads, all CONFIG.SYS records on the receiving terminal, both protected and non-protected (beginning with * or #), are retained. New CONFIG.SYS variables included in the download package, including the *GO variable, selectively replace existing variables with the same key name in the CONFIG.SYS file of the target group.
- All current passwords are retained on the receiving terminal during an application or operating system download (direct, by telephone, and back-to-back). This includes the system mode password and file group passwords. If required, you can replace existing *file group* passwords with new values as part of the data transfer operation.

NOTE

Always modify the *system mode* password in a separate, securely-controlled operation.

- For back-to-back application downloads, clear the RAM and flash of the receiving terminal before initiating the download. All application files stored on the receiving terminal, including CONFIG.SYS settings, are replaced by those of the sending terminal. System mode and file group passwords are retained on the receiving terminal.
- For full operating system downloads, Group 1 RAM is cleared as part of the operation and any application files stored in GID1 are erased. In this case, previously downloaded and authenticated applications must be downloaded again in a subsequent operation, together with the certificates and signature files required to authenticate them.

Set Up the Download Environment

The first step in performing a download to an Omni 37xx terminal is to establish the physical communication link between the sending and receiving system required to support the desired download method:

- Direct serial cable connection for direct application and OS downloads. The link is between the COM1 port of a download computer (PC) and the COM1 port on the receiving Omni 37xx terminal.

  Two special cables are available from VeriFone to support direct downloads: one for computers with DB25-type serial connectors (VPN 26263-02) and another for DB9-type connectors (VPN 26264-01). Both of these cables have a 10-pin RJ45 modular plug on one end for the terminal-side connection.

- Telephone line connection for application or OS downloads by telephone. The link is from the modem connection of a host computer to the integrated modem direct in the receiving Omni 37xx terminal.

  For this type of download operation, a standard telephone line cord with modular Telco connectors is required.

- Direct serial cable connection for back-to-back application downloads. The link is between the RS232 ports of the sending and receiving Omni 37xx terminals.

  A special cable is required for back-to-back downloads (VPN 05651-00). This cable has two 10-pin RJ45 modular plugs on each end to establish the terminal-to-terminal connection.

Cable Connection for Direct Downloads

There are two cables for direct downloads:

- DB25 serial connector (VPN 26263-02)
- DB9 connector (VPN 26264-01)

The following steps describe how to establish the cable link between the sending host computer and the receiving Omni 37xx terminal (see Figure 22):

1. Connect the DIN-type connector on one end of the cable to the COM1 (or COM2) serial I/O port on the download computer.
2. Connect the RJ45 connector on the other end of the download cable to the RS232 port on the back panel of the Omni 37xx terminal.

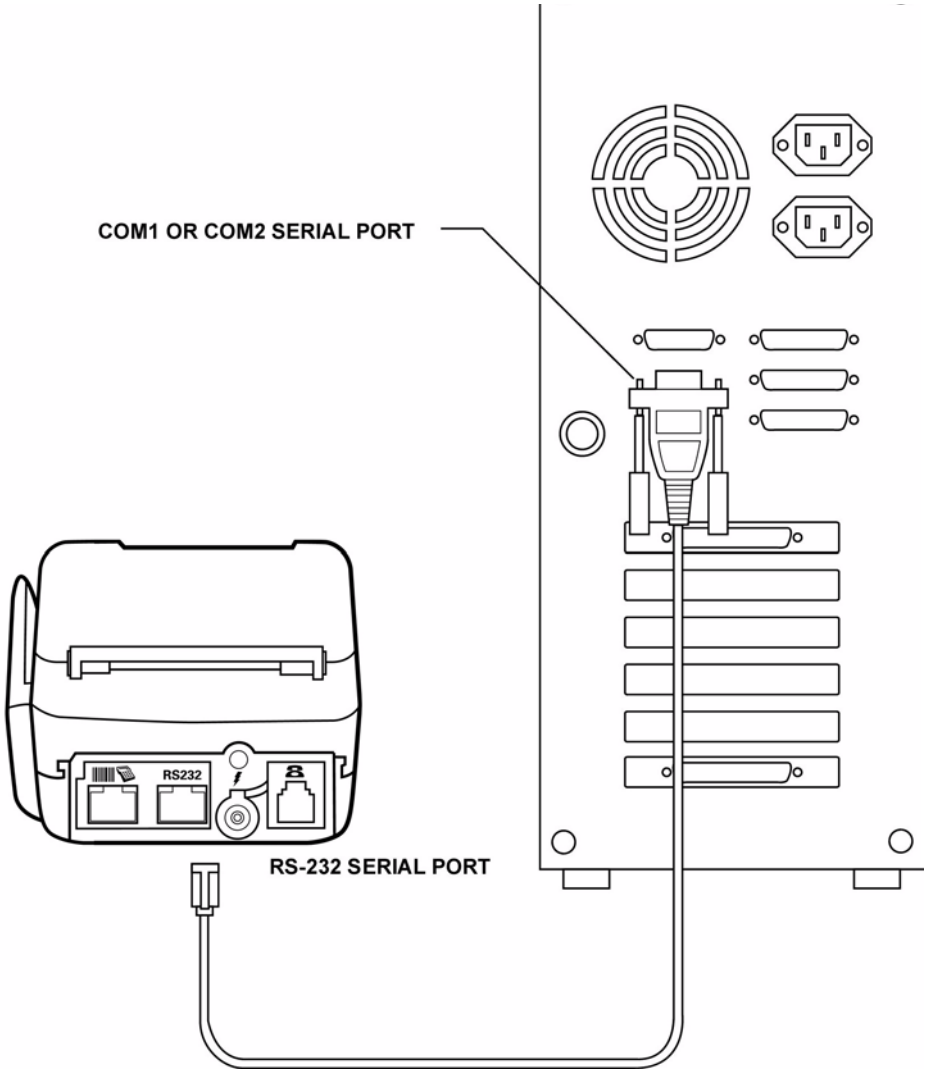


Figure 22 Serial Cable Connection for Direct Downloads

Telephone Line Connection for Telephone Downloads

To set up the telephone line connection for application or OS downloads between a host computer and an Omni 37xx terminal:

1. Confirm proper configuration of the dial-up telephone line and modem connection on the host computer.
2. Confirm the parameters for the download by telephone are set in the download tool.
3. Confirm that the receiving Omni 37xx terminal has a direct telephone line connection.
4. Ensure that the correct keyed variables used to control downloads by telephone are stored in the CONFIG.SYS file of the target file group on the receiving terminal.

Cable Connection for Back-to-Back Application Downloads

To prepare for a back-to-back application download:

1. Insert the RJ45 modular connector on one end of the download cable (VPN 05651-00) into the RS232 port of the sending terminal.
2. Insert the RJ45 connector on the other end of the cable into the RS232 port on the back panel of the receiving terminal.

Direct Application Downloads

This section provides procedures for direct downloads.

Hardware Checklist

- The correct cable connects the download computer serial port (COM1 or COM2) to the RS232 serial port (COM1) of the Omni 37xx terminal.

Software Checklist

- Download Manager, VeriCentre, or DDL.EXE running on the host computer.
- The application file to download (full or partial) resides on host computer.
- The correct keyed record variables exist in the CONFIG.SYS file(s) of the file group(s) to store the application files.
- Certificate files (*.crt) required for file authentication on the receiving terminal are stored in memory or they reside on the host computer and download together with the application files.
- All required signature files (*.p7s) generated using FILESIGN.EXE, reside on the host computer. One signature file downloads for each executable (*.out or *.lib) to run on the terminal.
- The filenames in the batch download list on the host computer indicate which application files to redirect to flash and file groups other than the target group.
- To avoid accidental overwrites, ensure that file names and CONFIG.SYS variables to download are correct in relation to those stored in memory of the receiving terminal.
- The required system mode and file group passwords are available to make the system mode menu selections required to prepare the receiving terminal to receive the application download.
- Sufficient memory space exists in RAM of the target group so that it can accept the entire download package, including certificates, signature files, and all data files.
- Use the system mode menu options to clear the entire RAM or flash or specific file groups on the receiving terminal (as necessary). Perform a flash defragment (coalesce) operation to optimize the flash file system (as necessary). (The application itself can issue a function call to defragment the flash on restart after the download.) For more information on system mode operations, refer to Chapter 4.

NOTE

Download, clear, and defragment operations cannot proceed in system mode if an application is executing. If you see the message DEVICE BUSY, PLEASE RESTART STAND ALONE, press the cancel key and restart the terminal from SYS MODE MENU 1. When you see the VeriFone copyright screen, enter system mode within 3 seconds (before the application starts).

Checklist for Effects on Files and Settings in the Receiving Terminal

- Protected records in the CONFIG.SYS file(s) of the receiving terminal — keyed records that begin with * or # — are not erased.
- The bootloader, OS, and other firmware on the receiving terminal are not modified as a result of the application download.
- The certificate tree that exists on the receiving terminal is not modified unless one or more new certificate files are downloading to the terminal. When new certificates are authenticated on the receiving terminal, the data they contain is stored in the certificate tree and the certificate files are deleted from the RAM of the target group.

Direct Application Download Procedure

The procedure in Table 21 describes how to perform a direct application download from a host download computer into the Group 1 application memory area of an Omni 37xx deployment terminal.

Steps described in the *Action* column are performed directly on the Omni 37xx terminal. Notes provided in this column indicate and explain actions you must perform on the host computer.

NOTE

The five steps listed in Table 21 are required for all download and upload procedures. In each of the following procedural tables, step numbering starts at 1 to indicate the unique steps of the specific download method. In subsequent procedures, only the method-specific steps are documented; the five steps in Table 20 are assumed to be completed.

Table 20 Common Steps to Start a Download

Step	Display	Action
1	VERIFONE OMNI Q50011A0 01/10/02 Verix COPYRIGHT (C) 1997-2003 VERIFONE, INC. ALL RIGHTS RESERVED	When the terminal restarts, a copyright screen displays that shows the version of Omni 37xx system firmware stored in the terminal's flash EPROM, the date the firmware was loaded into the terminal, and the copyright. This screen displays for three seconds, during which time you can enter system mode by simultaneously pressing F2 and F4. To extend the display period of this screen, press any key during the initial three seconds. Each key press extends the display period an additional three seconds.
2	(Application Prompt) or DOWNLOAD NEEDED	If an application already exists on the receiving terminal, the application starts and the application prompt displays. Otherwise, the DOWNLOAD NEEDED message displays. To enter system mode, simultaneously press F2 and F4.

Table 20 Common Steps to Start a Download

Step	Display	Action
3	SYSTEM MODE ENTRY PASSWORD ----------	Enter the system mode password. If an application already resides on the terminal, a unique system mode password may already exist. In this case, type that password and press enter to confirm your entry. If DOWNLOAD NEEDED displayed in step 2, enter the default password, "Z66831". To type this password on the keypad, enter: 1 ALPHA ALPHA 6 6 8 3 1, and then press enter. If you enter an incorrect password, the message, PLEASE TRY AGAIN displays. Reenter the password. To correct a typing mistake, press [←] to delete the entry, and retype your entry. To end the password entry session and return to the display shown in Step 2, press the cancel key.
4	SYS MODE MENU 1 CONTRAST F2 CLOCK F3 RESTART F4 ↓	When the system mode password is accepted, the terminal enters system mode and SYS MODE MENU 1 displays. To display additional system mode menus, press the PF2 key located on the terminal just below the on-screen down arrow. You can also press the enter key to toggle to the next menu. To perform any type of download operation, press the enter key one time when SYS MODE MENU 1 displays to move to SYS MODE MENU 2.
5	SYS MODE MENU 2 DOWNLOAD F2 RAM FILES F3 FLASH FILES F4 ↑↓	When SYS MODE MENU 2 displays, press F2 to select the DOWNLOAD menu option. To return to SYS MODE MENU 1, press the PF1 key located on the terminal keypad just below the on-screen up arrow. To return to SYS MODE MENU 1 and cancel the download procedure from within SYS MODE MENU 2, press the cancel key.

Table 21 Direct Application Download Procedure

Step	Display	Action
1	SYS MODE FILE FILE GROUP _1	Enter the target file group for the download. File Group _1 (Group 1) displays as the default selection. To select Group 1 as the target file group, press enter; to select a file group other than Group 1, type the one or two-digit number of the desired file group (2–15) for the download.
2	SYSTEM MODE FILE GROUP _1 PASSWORD ----------	Enter the password of the selected file group. For example, if Group 1 is the target group, the GROUP_1 PASSWORD message as shown at left displays. To continue, enter the required file group password and press enter to confirm your entry.
3	SYS MODE DOWNLOAD G _1 FULL F3 PARTIAL F4 ↑	Select if the download operation is FULL or PARTIAL. To perform a full application download, press F3; to perform a partial download, press F4. To return to SYS MODE MENU 2, press the PF1 key.

Table 21 Direct Application Download Procedure

Step	Display	Action
4	SYS MODE DOWNLOAD G _1 MODEM F2 COM1 F3 COM2 F4 ↑↓	Select the terminal port to use for the data transfer from the host computer to the receiving terminal. (To display additional menu options, press the PF2 key.) For a direct application download, always select the COM1 menu option by pressing F3. When you press F3, the terminal is ready to receive the application download from the host computer.
5	SYS MODE DOWNLOAD G _1 DOWNLOADING NOW	To initiate the download, execute the proper command(s) in the download tool running on the host computer. The data transfer operation starts, and the status messages shown at left display on the terminal screen. The progress of the download is indicated by a series of ten asterisks (each asterisk indicates 10% of the download is complete). When the last asterisk displays, the direct download is complete. You can stop the download operation at any time by pressing the cancel key. The terminal restarts automatically.
6	**VERIFYING FILES** CHECK CERTIFICATE (FILENAME.CRT) **AUTHENTIC** or else --- FAILED ---	When the download is complete, the terminal restarts automatically. The file authentication module on the receiving terminal begins to check for new certificate files (*.crt) and signature files (*.p7s) included in the download. These special files then process, one at a time; certificates are processed first, then signature files. When the file authentication module is invoked, the status display informs you of the progress of the file authentication process. If file authentication succeeds for a specific certificate, the "AUTHENTIC" message displays directly below the certificate filename. If file authentication fails for a specific certificate, the "FAILED" message displays for five seconds below the filename and the terminal beeps three times, allowing you to note which certificate failed to authenticate. The authentication process then continues to the next certificate until all new certificates are authenticated.

Table 21 Direct Application Download Procedure

Step	Display	Action
7	**VERIFYING FILES** COMPARE SIGNATURE FILENAME.P7S FILENAME.OUT **AUTHENTIC** or else --- FAILED ---	The file authentication module proceeds to authenticate any new signature files downloaded with the OS files. When the signature file authentication routine starts, the status display shown at left informs you of the progress of the authentication process. If file authentication succeeds for a specific signature file, the "AUTHENTIC" message displays directly below the filename of the signature file. If file authentication fails for a specific signature file, the "FAILED" message displays for five seconds below the filename and the terminal beeps three times, allowing you to note which signature file failed to authenticate. The authentication process then proceeds to the next signature file until all signature files are validated. When all new signature files are authenticated, the terminal restarts and the application specified in the *GO variable or the default application in Group 1, executes and starts running on the terminal.
8	(Application Prompt) or DOWNLOAD NEEDED	If the downloaded application successfully authenticated, the corresponding application prompt or logo displays on restart. The terminal can now process transactions. **Note:** The message DOWNLOAD NEEDED appears if: •The *GO variable is not set. •*GO does not specify an application is present. •The application did not authenticate (invalid or missing *.p7s file). •The application uses shared libraries that are missing or were not authenticated (invalid or missing *.p7s files). **Note:** If one or more executables in the application fail to successfully authenticate, the application may not run. If the application attempts to access an unauthenticated executable or library, it may crash. You must then repeat the direct download procedure using the correct certificates and/or signature files.

Direct Operating System Downloads

This section presents procedures for direct downloads.

Hardware Checklist

- The correct cable connects the download computer serial port (COM1 or COM2) to the Omni 37xx RS232 serial port (COM1) (refer to Cable Connection for Direct Downloads).
- Verify that the RAM size on the receiving terminal is large enough to receive files uploaded from the sending terminal. If the RAM on the sending terminal is 512 KB, the RAM on the receiving terminal must be at least 512 KB.

Software Checklist

- Download Manager, VeriCentre, or DDL.EXE running on the host computer.
- The complete OS version to download resides on host computer.
- Determine full or partial download of the OS. In a full OS download, the terminal restarts automatically and the new OS is processed, replacing the existing OS. In a partial OS download, the terminal returns to system mode and the new OS does not process until you manually initiate a terminal restart from system mode.
- The correct keyed record variables for the download exist in the CONFIG.SYS files of Group 1. (OS files must always download into GID1 RAM). The required variables can also be written into the CONFIG.SYS file as part of the download operation.
- The following files, provided by VeriFone CA for full OS downloads, must reside on the host computer:
  - The new OS version or OS update (Q*.out, 1*.out, 2*.out).
  - A signature file, called VFI.P7S, for the OS update. This signature file is generated by VeriFone CA using the high-level OS certificates for the Omni 37xx platform.
  - A file called VFI.PED. This file is an encrypted list of the new OS files.
  - One or more digital certificates (*.crt) download with the OS update.

  All new OS files, including VFI.P7S, VFI.PED, all certificate files, and any other files in the download package provided by VeriFone CA, must download together into Group 1 RAM.
- The required system mode and file group passwords are available to make the system mode menu selections required to prepare the receiving terminal to receive the OS download.
- Sufficient memory space exists in the Group 1 RAM to accept the OS download package including certificates, signature files, and all data files.

- Use system mode menu options to clear the entire RAM or the RAM of Group 1 on the receiving terminal (as necessary).

NOTE

Download, clear, and defragment operations cannot proceed in system mode if an application is executing. If you see the message DEVICE BUSY, PLEASE RESTART STAND ALONE, press the cancel key and restart the terminal from SYS MODE MENU 1. When you see the copyright screen, enter system mode within three seconds (before the application begins).

Checklist for Effects on Files and Settings in the Receiving Terminal

- A full OS download replaces the existing OS and erases all application files from the Group 1 RAM.
- A partial OS download returns control of the terminal to system mode and does not erase application files from Group 1 RAM.
- Protected records in the CONFIG.SYS file(s) of the receiving terminal — keyed records that begin with * or # — are not erased.
- An OS download does not overwrite terminal configuration settings, including the current date and time, passwords, and modem country code. If required, you can download new terminal configuration settings together with the OS files.
- The certificate tree that exists on the receiving terminal is not modified unless one or more new certificate files required to authenticate the new OS are being downloaded to the terminal. When new certificates are authenticated on the receiving terminal, the data they contain is stored in the certificate tree and the certificate files are deleted from the Group 1 RAM.
- The certificates and signature files required to authenticate the new OS are processed by the file authentication module of the receiving terminal the same as application files.
- When the terminal restarts and the new OS files are processed, they are moved out of the Group 1 RAM into the Group 0 area of the Omni 37xx file system.

Direct Operating System Download Procedure

The procedure in Table 22 describes how to perform a direct operating system download from a host computer into the Group 1 RAM of an Omni 37xx terminal.

Steps are performed directly on the Omni 37xx terminal. Notes provided in the Action column indicate actions to perform on the download computer side of the data transfer.

NOTE

In Table 22 and in the following procedures, only method-specific steps are included. For a description of the first five steps required to enter system mode and display SYS MODE MENU 2, please refer to Table 20.

Table 22 Direct Operating System Download Procedure

Step	Display	Action
1	SYS MODE FILE FILE GROUP _1	Enter the target file group for the download. File Group _1 (Group 1) is the default. Operating system files must *always* download into Group 1. This is the default group number in system mode. To select Group 1 as the target file group, press enter.
2	SYSTEM MODE FILE GROUP _1 PASSWORD ----------	Enter the password of the selected file group (Group 1) and press enter to confirm your entry.
3	SYS MODE DOWNLOAD G _1 FULL F3 PARTIAL F4 ↑	Select the OS download operation: FULL or PARTIAL. To perform a full OS download, press F3; to perform a partial OS download, press F4. To return to the previous system mode menu, press PF1.
4	SYS MODE DOWNLOAD G _1 MODEM F2 COM1 F3 COM2 F4 ↑↓	Select the terminal port to use for the data transfer from the host computer to the receiving terminal. (To display additional menu options, press PF2.) For a direct OS download, always select the COM1 menu option by pressing F3. When you press F3, the terminal is ready to receive the OS download from the host computer.
5	SYS MODE DOWNLOAD G _1 ********** DOWNLOADING NOW	Initiate the download by executing the proper command(s) in the download tool running on the host computer (when the receiving terminal is prepared to receive the direct OS download). The data transfer operation starts and status messages display on the terminal screen. The progress of the download is indicated by a series of ten asterisks (each asterisk indicates 10% of the download has completed). When the last asterisk displays, the direct download is complete. To stop the download operation, press the cancel key. The terminal restarts automatically.
6	**VERIFYING FILES** CHECK CERTIFICATE (FILENAME.CRT) **AUTHENTIC** or else --- FAILED ---	When the OS download is complete, the terminal restarts automatically. The file authentication module on the receiving terminal then checks for new certificate (*.crt) and signature (*.p7s) files included in the download. It processes these special files one at a time; certificates are processed first, then signature files. When the file authentication module is invoked, the progress of the file authentication process displays. If file authentication succeeds for a specific certificate, the "AUTHENTIC" message displays directly below the certificate filename. If file authentication fails for a specific certificate, the "FAILED" message displays for five seconds below the filename and the terminal beeps three times, allowing you to note which certificate failed to authenticate. The authentication process then continues to the next certificate until all new certificates are checked.

Table 22 Direct Operating System Download Procedure

Step	Display	Action
7	**VERIFYING FILES** COMPARE SIGNATURE FILENAME.P7S FILENAME.OUT **AUTHENTIC** or else --- FAILED ---	The file authentication module proceeds to authenticate new signature files downloaded with the OS files. When the signature file authentication routine begins, the progress of the authentication process displays. If file authentication succeeds for a specific signature file, the "AUTHENTIC" message displays directly below the filename of the signature file. If file authentication fails for a specific signature file, the "FAILED" message displays for five seconds below the filename and the terminal beeps three times, allowing you to note which signature file failed to authenticate. The authentication process proceeds to the next signature file until all signature files are validated. When file authentication is complete, the terminal either restarts automatically and begins processing the new OS (full download) or it returns control to system mode (partial download). If you are performing a partial download, the terminal does not restart until manually initiated by pressing F4 in SYS MODE MENU 1. If an application resides on the terminal following the OS download, it executes and starts running on restart. **Note:** Because a full OS download clears the RAM, all terminal applications and related certificate and signature files must download to the terminal when performing this type of download.
8	(Application Prompt) or DOWNLOAD NEEDED	If you performed a full OS download, the DOWNLOAD NEEDED prompt displays. At this point, you can perform a direct application download on the receiving terminal. If you performed a partial OS download and manually restarted the terminal, the application residing in the terminal (if any) executes. The application prompt displays on terminal restart, after OS processing, and the application starts running.

Download by Telephone

The procedure to perform an application or OS download by telephone is similar to that of direct application (see Table 21) and direct operating system downloads (see Table 22).

Hardware Checklist

- Set up the dial-up telephone line and modem connection on the host computer.
- Set up the direct telephone line connection on the receiving Omni 37xx terminal, as described in Establish Telephone Line Connections.

Software Checklist

- Download Manager or VeriCentre installed and running on the host computer. (DDL.EXE can only be used for direct downloads.)
- The information required to control the download by telephone is stored in the CONFIG.SYS file of the target group selected on the receiving terminal. Required settings for Download Manager and VeriCentre may include the following:
  - Dial-up numbers used to established the telephone line connection

- Baud rate settings for the data transfer
- Terminal ID
- Application ID
- Operating system name or serial number

NOTE

For detailed information about the setup requirements and download procedures for Download Manager and VeriCentre, please refer to the user documentation supplied by VeriFone with these software products.

Telephone Download Procedure

Press F2 (step 4 in Table 23) to select the MODEM port on the receiving terminal when the port selection options display (SYS MODE MENU 2). When you press F2, the internal modem in the receiving Omni 37xx terminal dials the host computer to request the download. When the host computer accepts the call, the download procedure is initiated by the host.

Table 23 Download by Telephone Procedure

Step	Display	Action
1	SYS MODE FILE FILE GROUP _1	Enter the target file group for the download. File Group _1 (Group 1) is the default. Operating system files must *always* download into Group 1. This is the default group number in system mode. To select Group 1 as the target file group, press enter.
2	SYSTEM MODE FILE GROUP _1 PASSWORD ----------	Enter the password of the selected file group (Group 1) and press enter to confirm your entry.
3	SYS MODE DOWNLOAD G _1 FULL F3 PARTIAL F4 ↑	Select the OS download operation: FULL or PARTIAL. To perform a full OS download, press F3; to perform a partial OS download, press F4. To return to the previous system mode menu, press PF1.
4	SYS MODE DOWNLOAD G _1 MODEM F2 COM1 F3 COM2 F4 ↑↓	Select the terminal port to use for the data transfer from the host computer to the receiving terminal. (To display additional menu options, press PF2.) For a download by telephone, you *must* select the MODEM F2 menu option. When you press F2, the terminal can receive the download from the host computer over the Telco port telephone line connection.
5	SYS MODE DOWNLOAD G _1 ********** DOWNLOADING NOW	Initiate the download by executing the proper command(s) in the download tool running on the host computer. The data transfer operation then starts, and status messages display on the terminal screen. The progress of the download is indicated by a series of ten asterisks (each asterisk represents 10% of the completed download). When the last asterisk displays, the direct download is complete. You can stop the download operation by pressing the cancel key. The terminal restarts automatically.

Table 23 Download by Telephone Procedure

Step	Display	Action
6	**VERIFYING FILES** CHECK CERTIFICATE (FILENAME.CRT) **AUTHENTIC** or else --- FAILED ---	When the OS download is complete, the terminal restarts automatically. The file authentication module on the receiving terminal then checks for new certificate (*.crt) and signature (*.p7s) files included in the download. It processes these special files one at a time; certificates are processed first, then signature files. When the file authentication module is invoked, the progress of the file authentication process displays. If file authentication succeeds for a specific certificate, the "AUTHENTIC" message displays directly below the certificate filename. If file authentication fails for a specific certificate, the "FAILED" message displays for five seconds below the filename and the terminal beeps three times, allowing you to note which certificate failed to authenticate. The authentication process then continues to the next certificate until all new certificates are checked.
7	**VERIFYING FILES** COMPARE SIGNATURE FILENAME.P7S FILENAME.OUT **AUTHENTIC** or else --- FAILED ---	The file authentication module proceeds to authenticate new signature files downloaded with the OS files. When the signature file authentication routine begins, the progress of the authentication process displays. If file authentication succeeds for a specific signature file, the "AUTHENTIC" message displays directly below the filename of the signature file. If file authentication fails for a specific signature file, the "FAILED" message displays for five seconds below the filename and the terminal beeps three times, allowing you to note which signature file failed to authenticate. The authentication process proceeds to the next signature file until all signature files are validated. When file authentication is complete, the terminal either restarts automatically and begins processing the new OS (full download) or it returns control to system mode (partial download). If you are performing a partial download, the terminal does not restart until manually initiated by pressing F4 in SYS MODE MENU 1. If an application resides on the terminal following the OS download, it executes and starts running on restart. **Note:** Because a full OS download clears the RAM, all terminal applications and related certificate and signature files must download to the terminal when performing this type of download.
8	(Application Prompt) or DOWNLOAD NEEDED	If you performed a full OS download, the DOWNLOAD NEEDED prompt displays. At this point, you can perform a direct application download on the receiving terminal. If you performed a partial OS download and manually restarted the terminal, the application residing in the terminal (if any) executes. The application prompt displays on terminal restart, after OS processing, and the application starts running.

Back-to-Back Application Downloads

This section presents procedures for back-to-back terminal downloads.

Hardware Checklist

- The correct serial cable connects the RS232 ports of the sending and receiving Omni 37xx terminals (refer to Cable Connection for Back-to-Back Application Downloads).
- Verify the RAM size on the receiving terminal is large enough to receive files uploaded from the sending terminal. If the RAM on the sending terminal is 512 KB, the RAM on the receiving terminal must be at least 512 KB.

Software Checklist

- The firmware version of the sending and receiving terminals must be identical or very similar.
- One or more complete, authenticated, application programs are stored in GIDs 1-15, RAM or flash, of the sending terminal. In this type of operation, *all* files stored in application memory of the sending terminal download to the receiving terminal.
- Before you initiate the download procedure, remember to select Group 1 as the target file group on both the sending and receiving terminals. The required system mode and file group passwords must also be available to make the required system mode menu selections on both terminals.
- The current CONFIG.SYS variables, date and time, and other terminal configuration settings on the sending terminal are those downloaded to the receiving terminal. Ensure your desired settings.
- All signature files required to authenticate the application files being downloaded to the receiving terminal are present in the RAM or flash file system of the sending terminal.
- The certificate tree of the sending and receiving terminal must be synchronized. That is, there can be no more than one revision difference between the certificate data currently stored in the memory of the sending and receiving terminals.
- If application files are downloaded to the receiving terminal in previous operations, use system mode menu options to clear the RAM and flash file systems of the receiving terminal before you initiate the back-to-back download procedure. This ensures a clean download.

NOTE

Download, clear, and defragment operations cannot proceed in system mode if an application has already started. If you see the message DEVICE BUSY, PLEASE RESTART STAND ALONE, press the Cancel (X) key and then restart the terminal from system mode Menu 1. When you see the copyright notice screen, enter system mode within three seconds (before the application begins).

Checklist for Effects on Files and Settings in the Receiving Terminal

- A back-to-back application download overwrites existing applications, libraries, or any other files stored in RAM of the receiving terminal.
- All CONFIG.SYS records and settings on the receiving terminal—protected and non-protected—are replaced with those of the sending terminal. Ensure that these are correct on the sending terminal before initiating the download.
- Passwords on the receiving terminal are retained.
- Certificates and signature files downloaded to the receiving terminal together with application files must be processed by the file authentication module on the receiving terminal on terminal restart after the back-to-back download.
- The OS software on the receiving terminal is not affected by a back-to-back application download. (OS files cannot be downloaded in a back-to-back operation.)
- An application upload does not overwrite the existing certificate tree on the receiving terminal. Any downloaded certificate files are authenticated and then added to the tree.

Back-to-Back Application Download Procedure

The back-to-back application download process consists of two main phases:

1. Preparing a *Gold* Omni 37xx terminal (transfers application files to the *Target* Omni 37xx terminal).
2. Downloading application files from the Gold terminal to a properly configured Target terminal.

Prepare Gold Terminal (PC-to-Terminal)

1. Configure a PC for an application download operation to the Gold terminal:
   - Set the *FA variable (if present in the application) to 1.
   - Ensure all certificates, *p7s files, applications, and other required files are present.
   - Ensure the download is exactly what you want your Target terminals to receive.
2. Configure the Gold terminal to receive an application download from a PC. From SYS MODE MENU 2, set Group 1 and the COM1 port to receive the download.
3. Connect a cable between the RS232 serial ports of the PC and the Gold terminal.
4. Initiate the file transfer on the PC.
5. From SYS MODE MENU 2 on the Gold terminal, select either a full or a partial download.

   The PC transfers files to the Gold terminal.

Download Application Files to Target Terminal

1. Configure a Gold terminal for an application download operation to a deployment terminal:
   - If the *FA variable (if present in the application) is set to 1, you can reset it to 0. For more information on the *FA variable, refer to the *Verix Programmer's Manual* (VPN 19733).
   - Ensure the download is exactly what you want your Target terminals to receive.
   - Ensure that previously authenticated files are not changed prior to the file transfer operation.
2. Configure the Target terminal to receive an application download from the Gold terminal. From SYS MODE MENU 2, set Group 1 and the COM1 port to receive the file transfer.
3. Connect a cable (VPN 05651-xx) between the RS232 serial ports of the Gold and Target terminals.
4. From any system mode menu on the Gold terminal, press [*] and enter the GID1 password to initiate the file transfer.
5. From SYS MODE MENU 2 on the deployment terminal, select either a full or a partial download. The Gold terminal begins to transfer files to the Target terminal.

Figure 23 illustrates these two phases and how they relate to each other.

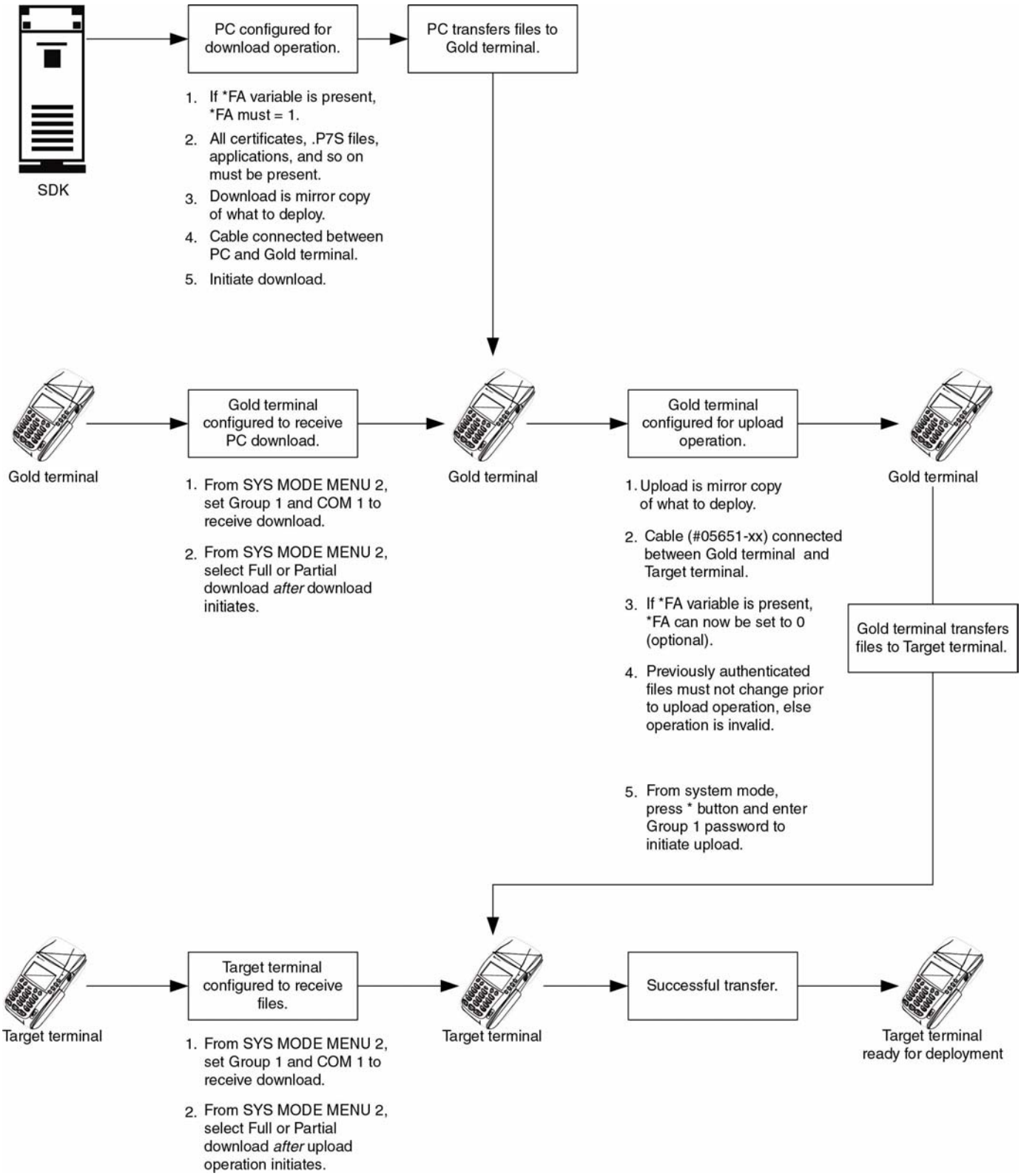

SDK
PC configured for download operation.
PC transfers files to Gold terminal.
1. If *FA variable is present, *FA must = 1.
2. All certificates, .P7S files, applications, and so on must be present.
3. Download is mirror copy of what to deploy.
4. Cable connected between PC and Gold terminal.
5. Initiate download.
Gold terminal
Gold terminal configured to receive PC download.
1. From SYS MODE MENU 2, set Group 1 and COM 1 to receive download.
2. From SYS MODE MENU 2, select Full or Partial download *after* download initiates.
Gold terminal
Gold terminal configured for upload operation.
1. Upload is mirror copy of what to deploy.
2. Cable (#05651-xx) connected between Gold terminal and Target terminal.
3. If *FA variable is present, *FA can now be set to 0 (optional).
4. Previously authenticated files must not change prior to upload operation, else operation is invalid.
5. From system mode, press * button and enter Group 1 password to initiate upload.
Gold terminal
Gold terminal transfers files to Target terminal.
Target terminal
Target terminal configured to receive files.
1. From SYS MODE MENU 2, set Group 1 and COM 1 to receive download.
2. From SYS MODE MENU 2, select Full or Partial download *after* upload operation initiates.
Target terminal
Successful transfer.
Target terminal ready for deployment

Figure 23 Back-To-Back Download Process

The procedure in Table 24 steps you through a back-to-back application download from a sending Omni 37xx terminal (Gold) to a receiving Omni 37xx terminal (Target).

Back-to-back downloads require that one terminal, the *Gold* terminal, be loaded with the required applications. The receiving terminal is the *Target* terminal. The procedure in Table 24 assumes the following:

- The Target terminal has no applications loaded.
- There is enough memory in the Target terminal to complete the download.

NOTE

The Target terminal does not display an error message if there is not enough memory to complete the download. However, the Gold terminal displays DOWNLOAD INCOMPLETE before returning to SYS MODE MENU 2.

- You are performing a *full* download.

Table 24 Back-to-Back Application Download Procedure

Step	Gold Terminal	Target Terminal
1	Connect a MOD10 cable (P/N 05651-XX) between the RS232 ports of the terminals. Allow each terminal to boot up. After boot up, the Target terminal displays DOWNLOAD NEEDED.	
2	Press F2+F4 to enter system mode.	
3	Enter system mode password (factory default is 1 ALPHA ALPHA 6 6 8 3 1[a]) and press the enter key.	
4	Press the ↓ key (PF2) to access the SYS MODE MENU 2 screen.	
5	Press the * (asterisk) key and press the Enter [↵] key. You are prompted to reenter the system mode password. UPLOADING NOW displays.	Press F2, DOWNLOAD, to enter download mode.
6		Press enter key at the next SYS MODE DOWNLOAD G _1 screen to select FILE GROUP_1 (default displayed) as the target file group.
7		Press F3, FULL, at the next SYS MODE DOWNLOAD G _1 screen. Full downloads are required in back-to-back downloads.
8		Select F3 (COM1) at next SYS MODE DOWNLOAD G _1 screen. DOWNLOADING NOW displays.
	Both terminals display a status indicator, where each dash represents a 10% increment of the download.	
	Ensure that the Gold terminal displays UPLOAD COMPLETE before returning to SYS MODE MENU 2. This is when the Gold terminal might display an error message if problems occurred during the download process.	
	The Target terminal begins to validate all files loaded. Allow the Target terminal to complete file authentication and reboot the terminal.	
	The Gold terminal is ready to perform another download. An application-specific menu displays after the Target terminal completes the reboot.	

a. Z66831; 1 ALPHA ALPHA = the character, Z.

Troubleshooting and Service

VeriFone follows stringent quality control standards in the manufacture of Omni 37xx terminals. Each unit that leaves the factory receives numerous tests to ensure quality and reliable operation. However, should you encounter a problem in operation, read this section for possible causes and solutions.

NOTE

Perform only those adjustments or repairs specified in this guide. For all other services, contact your local VeriFone distributor or service provider. Service conducted by parties other than authorized VeriFone representatives may void the product warranty.

NOTE

The Omni 37xx terminal comes equipped with tamper-evident labels. Do not, under any circumstance, attempt to disassemble the terminal.

Smart Card

The smart card implementation is a proprietary hardware solution that has no serviceable parts.

System Messages

Appendix A lists all system messages, including informational and error messages, and prompts, that may appear on the Omni 37xx display panel. For an explanation of a message that indicates some terminal malfunction occurred, please refer to the descriptions in Appendix A.

Use Remote Diagnostics to Identify Problems

Certain problems with a specific Omni 37xx terminal can be identified by a computer running a diagnostic test program. The diagnostic computer can be connected directly to a terminal by a cable or through a telephone line connection.

Troubleshooting Guidelines

The troubleshooting guidelines provided in the following section identify various problems and suggest appropriate corrective action(s). If you have problems operating your Omni 37xx terminal, please read through these troubleshooting examples. If the problem persists or if it is not described below, contact your local VeriFone representative for assistance.

Troubleshooting

During normal, day-to-day operation of your Omni 37xx terminal, it is possible that minor malfunctions may occur. Here are some examples of possible problems, and steps you can take to resolve them.

Terminal Display Does Not Show Correct or Readable Information

1. Check all cable connections and verify that the telephone line is properly connected.
2. Check display contrast by performing a local diagnostic test of the terminal display in system mode (refer to System Mode Menu 5).
3. If the problem persists, contact your local VeriFone representative for assistance.

Telephone Line Connection Does Not Work Properly

1. Check the telephone line cord and all telephone connections.
2. If you are using a pass-through (Telset) connection, check that the telephone handset is seated properly in its cradle. Also, check the line using another telephone. If the other telephone works, have the defective telephone repaired or replaced.
3. If you are using a direct (Telco) connection, check the Telco cable by plugging it into a working telephone and listening for a dial tone. If this test does not work, replace the Telco cable. If it is determined that the telephone line is dead, contact your local telephone company to check the status of the line.
4. If the problem persists, contact your local VeriFone representative for assistance.

Printer Does Not Work

1. Check if the printer is out of paper. Open the paper roll cover and install a new roll of printer paper.
2. Perform a test of the integrated thermal printer as described in System Mode Menu 2.
3. If the problem persists, contact your local VeriFone representative for assistance.

Serial Port Does Not Work

1. The serial port on the back panel of the terminal is identified by the RS232 icon. Check that the device connected to the serial port has power and is functioning properly. If possible, perform a self-test on the device in question.
2. The cable connecting the optional device to the terminal serial port may be defective. Try a different serial cable.
3. If the problem persists, contact your local VeriFone representative for assistance.

Terminal Does Not Process Transactions

There are several possible reasons why the terminal may not be operating properly or processing transactions. To check the most likely causes, follow the steps below.

Step 1: *Check the magnetic card reader*

1. Test the magnetic card reader as described in System Mode Menu 5.

2 Perform a test transaction using several different magnetic stripe cards to ensure the problem is not a defective card.

3 Make sure you are swiping cards properly. With the Omni 37xx card reader, the black, magnetic stripe on the card should face down, toward the keypad.

4 Process a transaction manually using the keypad instead of the card reader. If the manual transaction works, the problem may be a defective card reader. Contact your VeriFone distributor or service provider.

5 If the manual transaction does not work, proceed to Step 3.

Step 2: *Check the smart card reader*

1 Perform a test transaction using several different smart cards to ensure the problem is not a defective card.

2 Make sure you are inserting the cards properly. With the Omni 37xx smart card reader, the chip on the card should face down and inward.

3 Ensure the MSAM cards are properly inserted and the SAM holders are properly secured as described in Install/Replace MSAM Cards.

4 Process a transaction manually using the keypad instead of the card reader. If the manual transaction works, the problem may be a defective card reader. Contact your VeriFone distributor or service provider.

5 If the manual transaction does not work, proceed to Step 3.

Step 3: *Check the telephone line*

1 Connect to a working telephone and check for a dial tone. If there is no dial tone, replace the Telco cable.

2 If the problem appears to be with the telephone line, check with the party you are trying to call to see if their system is operational. If they are not experiencing difficulties with their line, contact the telephone company and have your line checked.

3 If the telephone line works, contact your local VeriFone representative for assistance.

Keypad Does Not Respond

1 Check the display panel. If it displays the wrong character or nothing at all when you press a key, follow the steps outlined in Terminal Display Does Not Show Correct or Readable Information.

2 If pressing a function key does not perform the expected action, refer to the documentation for that application to be sure you are entering data correctly.

3 Perform a local diagnostic test of the keyboard in system mode (refer to System Mode Menu 5).

4 If the problem persists, contact your local VeriFone representative for assistance.

Cleaning and Care

For normal dirt, use a clean cloth slightly dampened with water and a drop or two mild soap. For stubborn stains, use alcohol or an alcohol-based cleaner.

CAUTION

Never use thinner, trichloroethylene, or ketone-based solvents — they can deteriorate plastic or rubber parts. Do not spray cleaners or other solutions directly onto the keypad or display.

CAUTION

Do not attempt to clean the smart card reader. Doing so may void your warranty. For smart card reader service, contact your VeriFone distributor or service provider.

VeriFone Service and Support

For Omni 37xx terminal problems, contact your local VeriFone representative or service provider.

For Omni 37xx product service and repair information:

- (USA) VeriFone Service and Support Group, 1-800-834-9133, Monday–Friday, 8 A.M.–7 P.M. eastern time
- (International) Contact your local VeriFone representative

For Omni 37xx supplies:

- VeriFone Online Store at *www.store.verifone.com*
- (USA) VeriFone Customer Development Center, 1-800-233-0522, Monday–Friday, 7 A.M.–5 P.M. mountain time
- (International) Contact your local VeriFone representative

Returning a Terminal

Before returning an Omni 37xx terminal to VeriFone, you must obtain a Merchandise Return Authorization (MRA) number. The following procedure describes how to return one or more terminals for repair or replacement (U.S. customers only):

NOTE

International customers, please contact your local VeriFone representative for assistance with your service, return, or replacement.

1. Gather the following information from the printed labels (Figure 24) on the bottom of *each* Omni 37xx terminal you are returning:
   - Product ID, including the model and part number. For example, “OMNI 3750” and “PTID xxxxxxxx”
   - Serial number (S/N xxx-xxx-xxx)
2. Within the U.S., call VeriFone toll-free at 800-834-9133.
3. Select the MRA option from the automated message. The MRA department is open Monday–Friday, 8 A.M.–7 P.M., EST.
4. Give the MRA representative the information gathered in Step 1.

   If the list of serial numbers is long, you can fax the list, along with the information gathered in Step 1, to the MRA department at 502-329-5947.

- Please address the fax clearly to the attention of the “VeriFone MRA Dept.”
- Include a telephone number where you can be reached and your fax number.
- You will be issued MRA number(s) and the fax will be returned to you.
-

NOTE

One MRA number must be issued for each terminal you return to VeriFone, even if you are returning several of the same model.

5 Describe the problem and provide the shipping address to return the repaired or replacement unit.

6 Provide the shipping address where the repaired or replacement unit must be returned.

7 Keep a record of the following items:

- Assigned MRA number(s)
- VeriFone serial number assigned to the Omni 37xx terminal you are returning for service or repair (terminal serial numbers are located on the bottom of the unit (see Figure 24)
- Shipping documentation, such as airbill numbers used to trace the shipment
- Model(s) returned (model and part numbers are located on the bottom of each terminal)
- Model(s) returned (model numbers are located on the VeriFone label on the bottom of the Omni 37xx terminal)

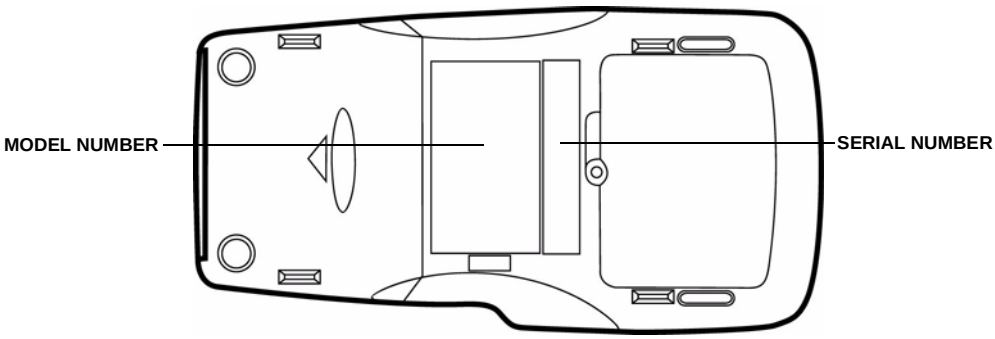


Figure 24 Information Labels on Bottom of Terminal

Specifications

Power

Omni 37xx terminal: 24 V DC; 1.5 A

DC Power Pack

For non-switching power supplies:

- UL, ITE listed, Class 2 power supply
  - Input rated: 110 - 127V AC, 60 Hz
  - Output rated: 24V DC 1.5 A

For switching power supplies:

- UL, ITE listed, Class 2, switching power supply
  - Input rated: 100 - 240 V AC, 50/60 Hz
  - Output rated: 24 V DC, 1.5 A

Barrel connector polarity:

Temperature

- Operating temperature: 0° to 40° C (32° to 104° F)
- Storage temperature: -18° to + 66° C (0° to 150° F)
- Relative humidity: 15% to 90%; no condensation

External Dimensions

- Length: 210 mm (8.3 in)
- Width: 104 mm (4.1 in)
- Depth: 83 mm (3.3 in)
- Weight: 760 gms (1.675 lb)

Weight

Terminal unit weight: 1.28 kg (2.82 lb)

Shipping weight: 3.26 kg (7.19 lb)

The shipping weight includes: shipping carton, terminal, power pack and cable, telephone line cable, one *Omni 37xx Certifications and Regulations*, and one *Omni 37xx Quick Installation Guide*.

Accessories and Documentation

VeriFone produces accessories and documentation for the Omni 37xx terminal, as listed below. When ordering, refer to the part number in the left column.

- VeriFone Online Store at www.store.verifone.com
- USA: VeriFone Customer Development Center, 1-800-233-0522, Monday–Friday, 7 A.M.–5 P.M., MST
- International: Contact your local VeriFone representative

Power Pack

Contact your local VeriFone distributor to determine which power pack or power cord fits your needs.

CPS05791-3A	DC power pack (universal)
21973-01	Power cable (US)

Thermal Printer Paper

CRM0039	High-grade thermal printer paper, 58-mm (2.25-inch) width, 25-meter (82-feet) length; single roll
CRM0039-01	CRM0039 in 30-roll bulk package
CRM0040	High-grade thermal printer paper, 58-mm (2.25-inch) width, 33-meter (108.26-feet) length; single roll

Paper Roll Spindle

02117-03	Plastic spindle for 58-mm (2.25-inch) rolls of thermal printer paper

VeriFone Cleaning Kit

02746-01	Cleaning kit

Download Cables

05651-xx	MOD10-MOD10 (terminal-to-terminal)
26263-xx	02xxx MOD10-PC DB25F (terminal-to-PC)
26264-xx	02xxx MOD10-PC DB9F (terminal-to-PC)

Cables for Optional Peripherals

07041-xx	MOD10-MDIN9 (CR 600/CR 1000*i* check readers; P250/P355/P900 external printers)
26519-xx	MOD10-MD8M (P950 external printers)
07042-xx	MOD10-4P4C (all VeriFone PINpads)

Telephone Line Cord

00124-17	2.1-meter (7-foot) telephone line cord, black, with modular RJ11-type connectors

Wire Clip

07826	Wire clip

Documentation

22429	*Omni 37xx Certifications and Regulations*
22398	*Omni 3750 Quick Installation Guide*
22407	*Omni 3740 Quick Installation Guide*
22409	*Omni 3720 Quick Installation Guide*
22408	*Omni 3710 Quick Installation Guide*
22403	*Omni 3705 Quick Installation Guide*
19733	*Verix Operating System Programmer's Manual*
22399	*Omni 37xx Series Installation Guide*
22410	*Omni 37xx Privacy Shield Quick Installation Guide*
22411	*Omni 37xx Swivel Stand Quick Installation Guide*
22413	*Omni 37xx Service Guide*
19733	*Verix Programmer's Manual*

System Messages

This appendix describes error and information messages that may appear when the Omni 37xx terminal is in system mode. For ease of use, these messages are grouped alphabetically.

These messages include those:

- displayed digital certificate and signature file download to the terminal
- processed by the file authentication module
- displayed when using the file compression module of the VeriCentre DMM terminal management and download tool

```
ALREADY DEBUGGING
```

This message displays when `DEBUGGER F4` in `SYS MODE MENU 4` is selected and the debugging monitor program, DBMON.OUT, is already running on the terminal.

```
APPLICATION
ALREADY RUNNING
PLEASE RESTART
```

This message displays when an attempt was made to invoke a system mode function not allowed to execute while an application is running on the terminal. The requested function is not invoked, and the application continues to run in the background.

Some system mode functions, such as setting the date and time, can be performed in this mode even with the application running in background, and this message does not display. For other system mode functions, such as downloads and RAM or flash clear operations, you must restart the terminal and re-enter system mode *before* the application starts (within three seconds).

To restart the terminal and enter system mode:

1. Press the cancel key until the `SYS MODE MENU 1` displays.
2. Select `RESTART F4`.
3. Enter system mode within three seconds of seeing the VeriFone copyright screen—before the application begins—by simultaneously pressing F2 and F4.

```
DEVICE BUSY
PLEASE RESTART
STAND ALONE
```

This message displays when a system mode function queried an internal device that is busy. This message can also occur if you entered system mode with an application running.

For example, if the application opened the magnetic stripe card reader and you try to invoke the card reader diagnostic through `MAG CARD READER F4` in `SYS MODE MENU 5`, the attempt fails and this message appears.

Restart the terminal and enter system mode before the application starts.

```
DOWNLOAD NEEDED
```

The operating system is unable to start the application specified in the *GO variable for the following reasons:

- No application resident in the terminal.
- The *GO variable is not set in the Group 1 CONFIG.SYS file.
- The application file specified in the *GO variable does not exist in Group 1. (The *GO variable cannot specify an application file stored in a file group other than Group 1.)
- The application or a shared library used by the application either does not exist or is not authenticated. All executables must be authenticated to run on the terminal.
- There is not enough memory available to run the application requested in the *GO variable.

```
FLASH CHKSUM ERROR
```

A corrupt file is detected in the flash file system during terminal start up, after power-on, or during restart. This message may indicate a hardware problem or the error condition may be resolved through another download of the file.

```
LOAD DBMON.OUT
```

The DEBUGGER F4 option in SYS MODE MENU 4 was selected. The debugging monitor program, DBMON.OUT, is included in the SDK, but is not stored in the terminal memory of a factory unit. To use the debugging tool, you must sign, download, and authenticate the DBMON.OUT application.

```
LOAD TERMINAL
MANAGEMENT AGENT
```

This message displays if you select REMOTE DIAGS F2 in SYS MODE MENU 4 and the (optional) Terminal Management Agent (TMA) software is not resident in the Omni 37xx terminal. The TMA software is required to perform remote diagnostics. For more information about support for remote diagnostics, contact your VeriFone service provider.

```
MODL
CTRY
KEYPAD
DISPLAY
MAG RDR
PRINTER
```

This message displays when you select CONFIG INFO F2 in SYS MODE MENU 3 and press the PF2 key (below the down arrow) two times. This third display, in a series of four, provides the following information about the current terminal configuration:

- MODL: The 12-digit model number assigned to the terminal on manufacture.
- CTRY: The name or abbreviation (up to 42 characters) of the country of manufacture.
- KEYPAD: A 1-digit code (0–5) to indicate keypad type.
- DISPLAY: A 6-digit code (000000, 000001, or xxxyyy) to indicate display unit type.
- MAG RDR: A 1-digit code (0–4) to indicate magnetic stripe card reader type.
- PRINTER: A 1-digit code (0 or 1) to indicate that a thermal printer is integrated.

```
PINPAD
LIFE
RSET
RCNT
MODEM CTRY
```

This message displays when you select CONFIG INFO F2 in SYS MODE MENU 3 and press the PF2 key (below the down arrow) three times. This fourth display, in a series of four, provides the following information about the current terminal configuration:

- PINPAD: A 1-digit code (0 or 1) to indicate that a PIN pad is integrated.
- LIFE: The number of seconds the terminal has run since first powered on.
- RSET: The date and time when the terminal was last reset, in *yymmddhhmmss* format.
- RCNT: The total number of times the terminal has been reset.
- MODEM CTRY: The current two-digit modem country code setting. For additional information about modem country codes, see the *Verix Operating System Programmer's Manual* (VPN 19733).

```
PLEASE TRY AGAIN
```

This message displays if you enter an incorrect system mode password or an incorrect file group password. Repeat the password entry and press the enter key.

```
RAM
FLASH
SERNO
PTID
PART
VERS
```

This message displays when you select CONFIG INFO F2 in SYS MODE MENU 3 and press the PF2 key (below the down arrow) to display the next screen. This second display, in a series of four, provides the following information about the current terminal configuration:

- RAM: The RAM (SRAM) size in kilobytes (KB).
- FLASH: The flash memory size in KB.
- SERNO: The 11-digit serial number assigned to the terminal on manufacture.
- PTID: The 8-digit permanent terminal ID assigned to the terminal on manufacture. If no PTID is assigned, the default value is "12000000."
- PART: A 12-digit part number assigned to the terminal on manufacture.
- VERS: A 2-digit hardware version assigned to the terminal on manufacture.

```
RAM CHKSUM ERROR
```

A corrupt file is detected in the RAM file system at terminal start up, after power-on, or during restart. This message may indicate a hardware problem or the error condition may be resolved through another download of the file.

```
RAM FILES
  INUSE
  AVAIL
FLASH FILES
  INUSE
  AVAIL
```

This message displays when you select CONFIG INFO F2 in SYS MODE MENU 3. This first display, in a series of four, provides the following information about the current terminal configuration:

- INUSE: The number of bytes of memory space currently being used in the RAM file system (RAM FILES) or the flash file system (FLASH FILES).
- AVAIL: The number of bytes of memory space currently available in the RAM file system (RAM FILES) or the flash file system (FLASH FILES).

```
RECEIVING NOW
```

In back-to-back downloads, the *Target* (receiving) terminal displays this message on data transfer initiation when pressing the asterisk key (*). To stop the upload, press the cancel key on either terminal (Gold or Target).

```
SYS MODE CLEAR
CLEARING FLASH
PLEASE WAIT
```

This message displays when you select FLASH FILES F4 in SYS MODE MENU 2 and select CLEAR GROUP_nn F2 or CLEAR ALL FILES F3 to clear files from the flash memory of a specific file group (Group 1–15) or from the entire flash memory. This message remains until the files either within the file group or all files in flash are deleted.

If you select CLEAR ALL FILES F3, only application file(s) stored in the flash-based file system—not the files stored in RAM—are erased.

```
SYS MODE CLEAR
CLEARING RAM
PLEASE WAIT
```

This message displays when you select RAM FILES F3 in SYS MODE MENU 2 and select CLEAR GROUP_nn F2 or CLEAR ALL FILES F3 to clear files from the RAM of a specific file group (Group 1–15) or from the entire RAM. This message remains until the files either within the file group or all files in RAM are deleted.

If you select CLEAR ALL FILES F3, only the application file(s) stored in RAM—not the files stored in flash—are erased. If you erase the main application stored in the RAM file system, the terminal displays DOWNLOAD NEEDED after the VeriFone copyright screen on terminal restart.

Note that clearing the RAM does *not* erase the keyed variable settings stored in protected CONFIG.SYS records—that is, in records that start with an asterisk (*).

```
SYS MODE DEFRAG
RECLAIMING FLASH
PLEASE WAIT
```

This message displays when you select FLASH FILES F4, followed by DEFRAG F4 in SYS MODE MENU 2 to perform defragmentation (coalesce) of the flash memory file system. PLEASE WAIT remains displayed during the defragmentation process. On successful completion, the terminal automatically restarts.

```
SYS MODE DOWNLOAD G _1
DOWNLOADING NOW
```

An application is being downloaded to a *receiving* Omni 37xx terminal from a host PC, either directly over a serial cable or by telephone. This message also displays on the Target terminal in a back-to-back download. The message also indicates the Group ID into which the application is being downloaded.

The terminal displays a series of asterisks (*) to indicate the progress of the download (each asterisk represents 10% of the file is downloaded). When ten asterisks appear, the data transfer is complete.

```
SYS MODE EDIT
FILE
KEY
VALUE
```

This message displays when you select EDIT F3 in SYS MODE MENU 3 to invoke the keyed file editor to edit files (such as, CONFIG.SYS), as follows:

- FILE: Make the appropriate menu selections to select or create a file to edit.
- KEY: Search for a specific keyed record.
- VALUE: Add a new value for a selected keyed record.

```
SYS MODE ERROR LOG
TYPE
FRAME
USP
TCB
TIME
```

This information appears when you select ERROR LOG F3 in SYS MODE MENU 4. The following information helps developers interpret the cause of the most recent unrecoverable software error that occurred on the terminal:

- TYPE: The error type code. For a description of error types (codes 2–11), refer to Chapter 4.
- FRAME: The value of the stack frame.
- USP: The value of the user stack pointer.
- TCB: The value of the task control block.
- TIME: The binary-coded decimal clock time when the last error occurred in *yymmddhhmmss* format.

If you report a system error to VeriFone, you may be asked to provide the information displayed in this screen. For detailed information about the error log function and the terms listed above, please refer to the *Verix Operating System Programmer's Manual* (VPN 19733).

```
SYS MODE KBD TEST
KEYCODE nn
```

This message displays when you initiate a local diagnostic test of the terminal keyboard through KEYBOARD DIAG F3 in SYS MODE MENU 5. When invoked, the decimal ASCII keycode of each key you press (test) appears to the right of KEYCODE. For example, pressing the 1 key on the terminal keypad displays the corresponding ASCII keycode, 31.

```
SYS MODE PASSWORD
FILE GROUP nn
GROUP nn PASSWORD
```

This message displays when you initiate the procedure for modifying existing system mode passwords through PASSWORDS F4 in SYS MODE MENU 3. Additional menu options display to let you change the password of a file group (F2) or the system mode password (F3).

```
SYS MODE PASSWORD
NEW
AGAIN
PASSWORD CHANGED
```

This message displays when you select PASSWORDS F4 in SYS MODE MENU 3 to modify the existing system mode password.

- NEW: Make the appropriate menu selections to enter the new password.
- AGAIN: Repeat the entry to confirm the new password.
- PASSWORD CHANGED: Displays when the new password is accepted.

```
SYS MODE UPLOAD
UPLOADING NOW
```

In a back-to-back download, the *Gold* (sending) terminal displays this message when you initiate an upload from the receiving terminal. To stop the upload, press the cancel key on either terminal.

```
TRK1:
TRK2:
TRK3:
```

When you invoke a local system mode diagnostic test of the magnetic stripe card reader, status information appears for data track (TRK1, TRK2, and TRK3) on a magnetic stripe card.

To perform this test, select MAG CARD DIAG F4 in SYS MODE MENU 5 and swipe a magnetic stripe card through the card reader:

- NO DATA or VALID DATA: A successful test of the magnetic-stripe card reader displays for each track. Actual data stored on data tracks does not display.
- An error condition generates one of the following error messages for each track with an error:
  - NO DATA
  - NO START
  - NO END
  - LRC ERR
  - PARITY ERR
  - REVERSE END

Press the cancel key to end the local diagnostic test of the card reader.

```
** UNZIP Error n
xxxxxx
yyyyyy
```

If you are using the file compression module in DMM, information similar to what is shown above appears when an error occurs during file extraction from a downloaded ZIP archive. Note the error number and error codes (xxxxx and yyyyy) and try to download the archive again.

```
UNZIP stuff.zip
myprog.out
mydata.txt
6x8.fon
10x14.fon
...
```

If you are using the file compression module in DMM, information similar to what is shown above appears when a compressed file archive downloaded to the terminal decompresses (unzipped), and the files extracted from the archive.

```
** VERIFYING FILES **
Check Certificate
(or System Certificate)

filename.crt

** Authentic **
(or ---Failed---)
```

This message displays when the file authentication module detects a new digital certificate, together with the filename of the certificate to authenticate, during a download to the Omni 37xx terminal. If the authentication is successful, `Authentic` displays; otherwise, `Failed` displays for five seconds and the terminal beeps three times to draw attention to the filename of the certificate that could not be authenticated.

This message remains on screen until all new certificates are checked, one by one. In special cases where system certificates are being installed, `System Certificate` displays instead of `Check Certificate`.

```
** VERIFYING FILES **
Compare Signature

myfile.p7s
myfile.out

** Authentic **
(or ---Failed---)
```

The file authentication module detected a new signature file, together with the application file for which the signature file was generated, during a download to the Omni 37xx terminal. If the authentication is successful, `Authentic` displays; otherwise, `Failed` appears for five seconds and the terminal beeps three times to draw attention to the filename of the certificate that could not be authenticated.

This message remains on screen until all new signature files are checked. New digital certificates are always checked first, followed by new signature files, in an uninterrupted process.

ASCII Table

An ASCII table for the Omni 37xx display is presented as Figure 25 below. The table is formatted for quick reference, as follows:

- The letters and numbers in the column to the left of the table and in the row above the table are, when combined, the hexadecimal value of an ASCII character located in the corresponding row and column coordinate.
- The numbers shown in white on a black background within the table itself are the decimal value of the ASCII character in that table cell.
- The large character located in the middle of each cell is the ASCII character.

For example, to determine the hexadecimal value of the plus (+) sign:

1. Locate the plus sign ASCII character in the table (decimal 43).
2. From this position, follow the row to the left and view the hexadecimal value in the column outside the table. This value (2) is the first character of the ASCII character's hexadecimal value.
3. Now, from the plus sign, follow the column to the top of the table and view the hexadecimal value in the row above the table. This value (B) is the second part of the hexadecimal value.
4. The hexadecimal value for the ASCII plus sign (+) is therefore 2Bh.

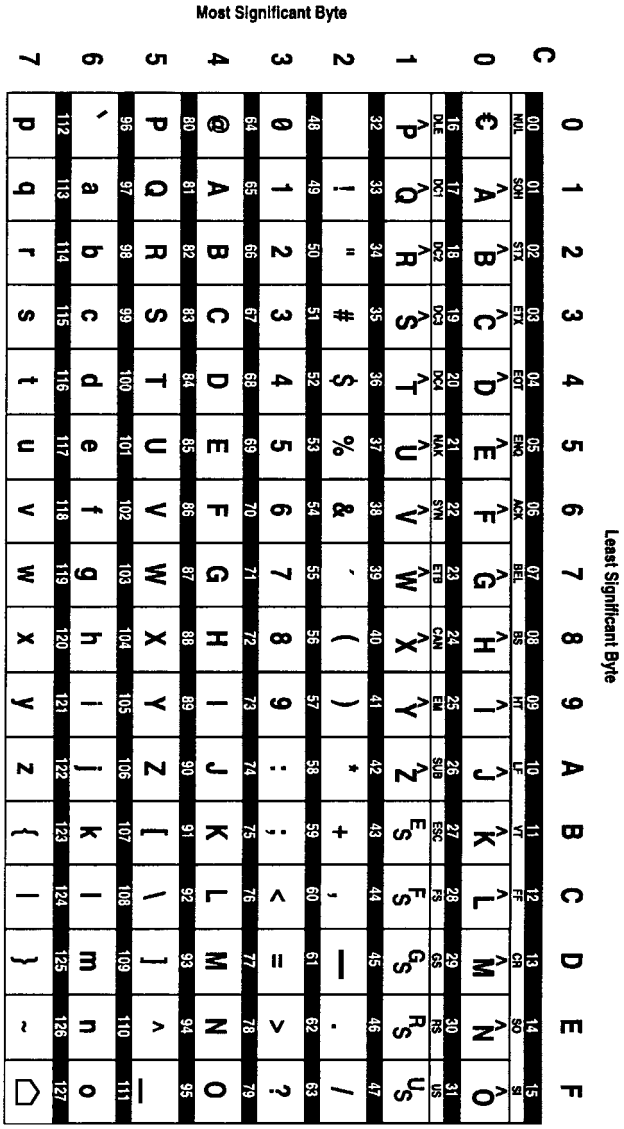
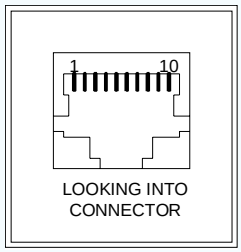

Most Significant Byte
Least Significant Byte
C
0 1 2 3 4 5 6 7 8 9 A B C D E F
0 NUL SOH STX ETX EOT ENQ ACK BEL BS HT LF VT FF CR SO SI
1 DLE DC1 DC2 DC3 DC4 NAK SYN ETB CAN EM SUB ESC FS GS RS US
2 ! " # $ % & ' ( ) * + , — . /
3 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
4 @ A B C D E F G H I J K L M N O
5 P Q R S T U V W X Y Z [\ ] ^ _
6 ` a b c d e f g h i j k l m n o
7 p q r s t u v w x y z { | } ~

Figure 25 ASCII Table for the Omni 37xx Display

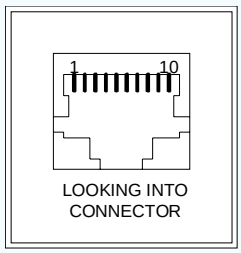
Port Pinouts

The tables in this appendix list pinouts for the Omni 37xx connectors.

PIN Pad Serial Port

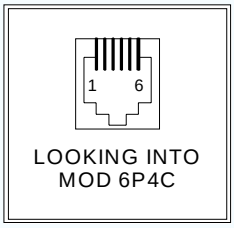
Connector	Pin	Function	Description
	1	BCIN	Receive data (TTL)
	2	VPINpad	+9V DC regulated power
	3	NC	No connection
	4	NC	No connection
	5	GND	Power ground
	6	/RXD	Receive data
	7	/TXD	Transmit data
	8	NC	No connection
	9	NC	No connection
	10	VCC_BC	+9V DC regulated power

RS232 Port

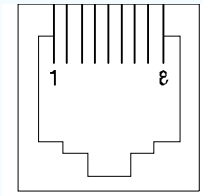
Connector	Pin	Function	Description
	1	TXCLK	Transmit clock signal
	2	NC	No connection
	3	CD	Carrier detect
	4	NC	No connection[a]
	5	GND	Power ground
	6	/RXD	Receive data
	7	/TXD	Transmit data
	8	CTS	Clear to send
	9	RTS	Request to send
	10	RXCLK	Receive clock signal

a. In most Verix terminals, Pin 4 of the RS232 port provides a Data Terminal Ready (DTR) signal. Omni 37xx terminals handle this pin differently, with no connection (NC).

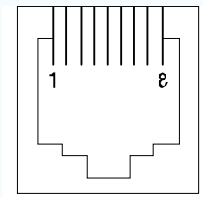
Telco Port

Connector	Pin	Function	Description
	1	NC	No connection
	2	NC	No connection
	3	Tip	Telephone line
	4	Ring	Telephone line
	5	NC	No connection
	6	NC	No connection

Ethernet Port

Connector	Pin	Function	Description
	1	TXD+	Transmit data +
	2	TXD-	Transmit data -
	3	RXD+	Receive data +
	4	NC	No connection
	5	NC	No connection
	6	RXD-	Receive data -
	7	NC	No connection
	8	NC	No connection

ISDN Port

Connector	Pin	Function	Description
	1	NC	No connection
	2	NC	No connection
	3	STA	Signal Transmit A
	4	SRA	Signal Receive A
	5	SRB	Signal Receive B
	6	STB	Signal Transmit B
	7	NC	No connection
	8	NC	No connection

Barrel Connector Polarity

Access code A code number dialed to gain access to a telephone line, such as dialing the number 9 to reach an outside line.

Application ID An alphanumeric code that identifies an application program downloaded to a terminal from a download computer. For VeriCentre application downloads, the application ID is stored in the CONFIG.SYS record which begins with the *ZA key. An Omni 37xx application ID can be up to 21 characters long. For VeriCentre Download Management Module, the application ID, as well as other CONFIG.SYS variables, may differ from those used for VeriCentre.

Application program The ordered set of programmed instructions by which a computer performs an intended task or series of tasks.

Application prompt The information shown on the terminal's display panel when power is applied to the terminal, assuming that an application program has already been downloaded into the terminal's memory and authenticated by the file authentication module. The application prompt often contains a graphical logo, and date and time, but it can consist of anything the programmer chooses for that purpose.

ASCII Abbreviation for *American Standard Code for Information Interchange*. A 7-bit code (with no parity bit) that provides a total of 128 bit patterns. ASCII codes are widely used for information interchange in data processing and communication systems.

Back-to-back application download The process of copying the contents of one terminal's application memory to another terminal's application memory. A terminal-to-terminal application upload require that the sending and receiving terminal be connected to each other by a serial cable. The same operation as a *terminal-to-terminal* application upload."

Bar code Optical binary code imprinted on merchandise in retail stores. To support specific applications, an optional bar code reader can be attached to the Omni 37xx to read and process bar codes.

Bar code reader A pencil- or wand-shaped optical scanner used to read bar codes. To read the code, you drag the tip of the bar code reader across the length of the bar code, in a left-to-right or right-to-left direction.

Baud The number of times per second that a system, especially a data transmission channel, changes state. The state of a system may represent a bit, digit, or symbol. For a POS terminal, the baud rate indicates the number of bits per second that are transmitted or received by the terminal's serial ports and modem.

Bit Short for *binary digit*. Either of the two digits 0 and 1 in the binary number system. Also, a unit of information equal to one binary decision. The bit is the smallest unit of storage and hence of information in any binary system within a computer.

Block A collection of data units such as words, characters, or records (generally more than a single word) that are stored in adjacent physical positions in memory or on a peripheral storage device. A block can therefore be treated as a single unit for reading, writing, and other data communication operations.

Boot loader Also called a *bootloader* or *bootstrap loader*. A short program, stored in flash EPROM, that allows the terminal to continue operating during an operating system download procedure, until the new operating system is downloaded into terminal memory.

Buffer A temporary memory for data, normally used to accommodate the difference in the rate at which two devices can handle data during a transfer.

Byte A term developed to indicate a measurable number of consecutive binary digits that are usually operated on as a unit. For the Omni 37xx, a byte consists of eight bits. See also Bit.

Calendar/clock chip A microchip inside the Omni 37xx terminal which keeps track of the current date and time.

Card reader Also called *magnetic stripe card reader*. The slot on the right side of the Omni 37xx terminal that automatically reads data stored in the magnetic stripe on the back of a specially-encoded card when you swipe the card through the slot.

Carrier Usually, an analog signal that is selected to match the characteristics of a particular transmission system. The carrier signal on a phone line is modulated with frequency or amplitude variations to allow a terminal to transmit or receive data using a modem. A carrier signal transmits data from a host computer to an Omni 37xx terminal over an analog telephone line.

Certificate Also called a *digital certificate*. A digital document or file that attests to the binding of a public key to an individual or entity, and that allows verification that a specific public key does in fact belong to a specific individual.

Character An element of a given character set. The smallest unit of information in a record. A letter, numeral, or other symbol to express information.

CONFIG.SYS file A special keyed file that is stored in terminal memory and which contains system and application configuration parameters. Each record in a CONFIG.SYS file is identified by an alphanumeric search key. In the Omni 37xx file system, there is one password-protected CONFIG.SYS file per file group (Groups 1–15). You can modify CONFIG.SYS records using the keyed file editor. See Keyed file editor.

CPU Abbreviation for *central processing unit*. The principal operating part of a computer system that controls the interpretation and execution of instructions stored in memory.

Data Information prepared, often in a particular format, for a specific purpose. Data is to be distinguished from applications or program instructions. In the Omni 37xx terminal, application files and data files can be stored in RAM or flash memory.

Data entry The process of using a keyboard, card reader, or other device to input data directly into a system.

Data packet A group of bits of fixed maximum size and well-defined format that is switched and transmitted as a composite whole through a packet switching network. Any message that exceeds the maximum size is partitioned and carried as several packets. Data packets are formed by the controller in the sending data terminal and the data is extracted and reassembled by the controller at the receiving end.

Dedicated line A leased or private telephone line that is used for a particular communications purpose, such as to connect an Omni 37xx terminal to a host computer. See Leased line.

Default A value, parameter, option, or attribute that is assigned by the program or system when another has not been assigned by the user.

Delete To remove a record, field, or item of data.

Diagnostics Techniques employed for detection and isolation of malfunctions and errors in programs, systems, and devices. In a diagnostic test, a program or routine is run to detect failures or potential failures. These tests and routines help detect and isolate problems in a terminal or peripheral device.

Dial-up line A standard public telephone line. The switching equipment on a dial-up line requires that a party dial the other party before a connection can be made.

Direct download The process of transferring files and/or data from a download computer to a terminal over a serial cable connection and in a local, as opposed to a remote, system environment.

Display The small screen on the Omni 37xx terminal that shows numerals, letters, and punctuation symbols in selected fonts, graphics in various formats, information entered from the keypad, as well as system prompts and messages.

Download To transfer files or data from a host computer or sending terminal over a communication link to a receiving terminal.

DTMF *Dual-tone multi-frequency*. The ordinary dial tone on a telephone line.

File authentication A process through which one proves and verifies the origin of a file, the identity of the sender, and the integrity of the information it contains.

Firmware System software, including the operating system, boot loader, default display font, and system messages, stored in terminal flash memory.

Fixed prompt A system prompt or message stored as part of system firmware in terminal memory. Fixed prompts appear on the terminal display to alert the user to specific system occurrences or malfunctions, and to prompt the user to enter specific information or select options.

Flash memory An area of non-volatile memory where files can be stored. The Omni 37xx also has a RAM-based file system. Files can be stored in RAM (drive `I:`) or in flash (drive `F:`) memory area of any file group (Groups 1–15).

Host computer Also called a *download* computer. The primary or controlling computer in a multiple computer operation. Also, a computer—usually a PC running Windows NT or Windows 95 or 98—used to prepare programs for download to POS terminals. Host computers are also used to process transactions that originate from a distributed network of POS terminals.

Input The process of entering data into a processing system or a peripheral device such as a terminal, or the data that is entered.

Interface A common boundary between two systems, devices, or programs. Also, to interact.

Keyed file character set A limited set of 95 ASCII characters, from 00h to 5Fh (or 0 to 95 decimal), that is used by the Omni 37xx keyed file editor. Although an application program can download all 95 characters in this set, you can only enter 50 of these characters from the terminal keypad: 0–9, A–Z, and 14 special characters.

Keyed file editor A keyed file editor lets you create new records or modify existing records stored in a keyed file such as CONFIG.SYS. See CONFIG.SYS file.

Keyed file record ASCII data, or variables, stored in the terminal's CONFIG.SYS file(s). A keyed file record consist of two parts: a search key that identifies the record, and the data or variable stored in the record. See CONFIG.SYS file.

Keypad A small keyboard or section of a keyboard containing a smaller number of keys, generally those used in simple calculators. The 16-key core keypad of the Omni 37xx terminal is used to enter data and perform operations.

Leased line A private telephone line leased from the phone company. See Dedicated line.

Line cord A telephone-type cord with modular plugs on each end to connect the terminal to a dial-up telephone line.

Local functions Operations performed at the terminal only and not in interaction with a host computer. For the Omni 37xx, local functions such as internal diagnostics are performed in system mode. See Chapter 4.

Manual transaction A transaction involving the manual entry of account information from the terminal keypad instead of automatic entry of the information from a reading device, such as a magnetic stripe card reader.

Memory A device or medium that can retain information for subsequent retrieval. The term is most frequently used to refer to the internal storage of a computer (or a terminal) that can be directly addressed by operating instructions. In the Omni 37xx, files can be stored in battery-backed RAM or in non-volatile flash memory.

Messages Words and symbols appearing on the display screen which inform the user of the terminal of the result of a process, or if an error has occurred. The term "prompt" is used when the displayed message is requesting the user to enter information or to select an option.

Modem *Modulator/demodulator*. A device that converts a digital bit stream into an analog signal to transmit over an analog communication channel (modulation), and converts incoming analog signals into digital signals (demodulation). The Omni 37xx terminal's internal modem allows communication with a host computer over a dial-up telephone line.

Non-volatile memory A memory or storage medium that retains data in the absence of power so that the data is available when power is restored. For the Omni 37xx, application files and data files can be stored in battery-backed RAM or non-volatile flash memory, according to the requirements of the application.

Normal Mode The operating mode for normal transaction processing. The main application (downloaded and authenticated) starts and displays an application prompt, indicating that the terminal is in normal mode. In this mode, the terminal is ready to process transactions. See also System Mode.

Packet A group of bits of fixed maximum size and well-defined format that is switched and transmitted as a composite whole through a packet switching network. Any message that exceeds the maximum size is partitioned and carried as several packets.

Packet-switched networks Networks of computers or computing devices in which communication resources are allocated dynamically on a variety of levels to multiple communicating entities. Messages between entities are partitioned into segments, or packets, with a fixed maximum size.

Parameter A variable that is usually assigned a constant value for a specific subroutine, procedure, or function. Parameters stored in terminal memory or in the CONFIG.SYS file(s), enable a host or download computer to identify to terminal configuration.

Password A group of characters that identify a user to the system so that they can gain access to the system or part of that system. Passwords are used to ensure the security of computer systems by regulating the amount of access freedom. The password used to enter system mode is called the *system mode password*. In the Omni 37xx file system, each file group (Groups 1–15) also has its own password.

PC Abbreviation for personal computer. Usually, PC refers to an IBM-compatible personal computer.

Peripheral device In a computer system, any equipment that provides the processing unit with outside communication. Typical peripheral devices for a POS terminal include PIN pads, bar code wands, and check readers.

Port An opening or connection that provides electrical or physical access to a system or circuit. Also, a connection point with associated control circuitry that allows I/O devices to be connected to the internal bus of a microprocessor.

POS terminal A terminal used at the *point of sale*, which is usually at a merchant site where a customer pays for goods or services received. Information concerning the sale can be entered into the terminal and transmitted to a remote host computer for verification and processing.

Power pack A unit for transforming and converting electrical power from one AC voltage level to another AC voltage level, or from AC to DC, for electronic devices.

Prompt A short message, sent from a process to a user, indicating that the process expects the user to present fresh data. For example, a prompt appears on the terminal display asking the user to enter specific information. See Messages.

Protocol An agreement that governs the procedures used to exchange information between cooperating entities. For example, protocols govern the format and timing of messages exchanged between devices in a communication system, such as between a terminal and a host computer.

PTID *Permanent terminal ID*. An optional identifier that can be permanently assigned to a VeriFone terminal at the factory, upon customer request. The PTID has two parts: a 2-digit manufacturer ID (12 for VeriFone) and a unique 8-digit terminal ID. If no PTID is assigned, the default PTID value is 1200000000.

Pulse dialing A method of telephone dialing that specifies a phone number by the number of electrical pulses sent.

RAM *Random-access memory*. The type of memory in which storage locations are addressable and can therefore be accessed in any order. In the Omni 37xx terminal, the RAM (or SRAM) is commonly used to store applications and temporary data generated during a transaction.

The RAM is battery-backed, meaning that if power is turned off, data stored in this area of volatile memory is not lost. Application files and data can also be stored in the non-volatile flash memory system. By default, files downloaded to the terminal are stored in the RAM of the target file group(s). The RAM file system is called drive `I:`. See Flash memory.

Remote host computer A host computer connected to a Omni 37xx terminal over a dial-up telephone line to download files or data, or to process transactions. The opposite of remote is *local*.

RS232 Also RS-232C. A widely used standard interface that covers the electrical connection between data communication equipment, such as a modem, and data terminal equipment, such as a microcomputer or computer terminal. The RS232 interface standard was developed by the EIA (Electronic Industries Association) and is essentially equivalent to the CCITT's V.24 interface.

Scroll To move all or part of the information displayed on a screen up or down, left or right, to allow new information to appear. For the Omni 37xx, text that does not fit entirely within the display area can be scrolled to the left or right using the pound (#) and asterisk (*) keys.

Search key Also called *key*. In the Omni 37xx, a short character string used by an application to identify a keyed file record stored in CONFIG.SYS file(s). For example, *ZA or *OT. A *keyed file record* consist of two parts: a search key to identify the record, and the variable data stored in the record. See also Keyed file record and CONFIG.SYS file.

Serial port A connection point through which digital information is transferred one digital bit at a time. Same as *serial interface*. The Omni 37xx terminal has one serial port, labeled RS232. The main serial port on a download computer is usually assigned the device ID, COM1.

Signature file A digital file with the filename extension *.p7s generated in an industry-standard format by the file signing tool, FILESIGN.EXE. The output of the file signing tool is a signature file in an industry-standard format.

SRAM See RAM.

Subroutine A software routine that can be part of another routine. When a main routine calls a subroutine, program control is transferred to the subroutine. When the subroutine is completed, control reverts to the instruction in the main routine immediately following the subroutine call.

Swipe The action of sliding a magnetic stripe card through a terminal card reader. The Omni 37xx card reader has a bi-directional swipe direction. The user must hold the card so that the magnetic stripe is faces in and towards the keyboard.

System Mode For the Omni 37xx, system mode temporarily disables normal mode operations, allowing you to perform local functions such as downloads, diagnostics, and other operations that cannot be performed while the application program is running.

At startup, the terminal displays a copyright notice screen that shows the version of Omni 37xx system firmware stored in terminal flash memory, the date it was loaded into the terminal, and the copyright notice. This screen appears for three seconds. To enter system mode, simultaneously press the F2 and F4 keys during this three-second period. Pressing any other key(s) during that period resets the copyright notice screen to display an additional three seconds.

See also Local functions and Normal Mode.

System mode password A unique set of characters entered by the user to access the system mode local functions of the terminal. A default password is supplied with each terminal. For the Omni 37xx terminal, the default system password set at manufacture is: Z66831.

To prevent unauthorized access, change the default password to a confidential password on terminal deployment. Store the new password in a safe place, as it is impossible to restore the terminal default password without sending the unit to VeriFone for service.

Telephone download The process of transferring an application program and/or data from a remote host or download computer to a terminal over a telephone line.

Telephone jack Also, telephone line wall jack. Insert a modular connector into a telephone jack or receptacle. Also, modular-type sockets for connecting telephone line cords. The Omni 37xx terminal has a TELCO RJ45-type telephone jack on the back panel used for a direct connection to a telephone line wall jack.

Telephone line The standard telephone wiring connecting your phone or terminal to a local or private telephone company.

Terminal Any device capable of sending and receiving data over a data link, such as a telephone line or a RS232 cable. Some terminals, such as the Omni 37xx, can print receipts and display information and graphics on a screen.

Terminal ID An alphanumeric code that identifies a terminal to a download computer. In this way, the download computer can determine what data or application programs to download to that terminal. For VeriCentre downloads, the Omni 37xx terminal ID is stored in the *ZT record in the CONFIG.SYS file. This variable should not exceed 10 characters in length. Not the same as PTID

Terminal-to-terminal application upload The process of copying the application memory contents of one terminal to the application memory of another terminal. A terminal-to-terminal application upload requires that the terminals be connected to each other by a serial cable. See also Back-to-back application download.

Tone dialing Also called *touch-tone dialing*. A method of telephone dialing that uses different pitched tones to specify a phone number. See also DTMF.

Track 1, 2, or 3 data Information stored on tracks 1, 2, or 3 of a debit or credit card magnetic stripe, which can be read by a magnetic card reader device, such as the one that is integrated in the Omni 37xx terminal.

Transaction An exchange of data resulting in a transfer of goods, services, value, and/or information between two parties.

Variable A string of characters that denotes some value stored within the computer and that can be changed during execution. A variable may be internal to a program, in which case it is held in memory, or external if the program must perform an input operation to read its value. See Parameter.

Volatile memory A type of memory where the contents are destroyed if the power supply to the memory is interrupted. When volatile memory, such as SRAM, is used for crucial applications, it is often back up by battery-supplied power. Compare with Non-volatile memory.

INDEX

A

Accessories **123**
- Ordering **123**

accessories
- cables for optional peripherals **123**
- documentation **124**
- download cables **123**
- ordering **123**
- paper roll spindle **123**
- power packs **123**
- telephone line cord **123**
- thermal printer paper **123**
- VeriFone cleaning kit **123**

application debugging **49**

B

back-to-back downloads **79, 80**
- file authentication **96**
- redirect files during **90**
- set up environment **99**

bar code wand
- connect **24**

C

cables
- ordering cables for optional peripherals **123**
- ordering download cables **123**

certificates and signature files **90**
check readers **24**
clear all flash files **42**
clear RAM **42**
clear smart card **69**
clock **40**
CONFIG.SYS files **48**
connect
- bar code wand **24**

D

Data entry modes
- Normal Mode **28**
- System Mode **28**

date and time **40**
- determine last reset **45**

DDL.EXE **80**
debugging **51**
debugging applications **49**
defragment flash **42**
defragment flash memory **40**
Diagnostics
- For troubleshooting **117**

diagnostics **51**
direct downloads
- cable connections **99**

direct telephone line connection **19**
Display
- Troubleshooting **118**

display contrast **39**
display panel test **51**
Documentation **123**
documentation, ordering **124**
download cables, ordering **123**
Downloads
- Definition of the term "download" **141**
- Performing a direct application download
  - Checklist for effects on files and settings in the receiving terminal **102**
  - Hardware checklist **101**
  - Procedure **102**
  - Software checklist **101**
- Performing back-to-back application downloads
  - Checklist for effects on files and settings in the receiving terminal **113**
  - Hardware checklist **112**
  - Procedure **113**
  - Software checklist **112**
- Performing direct operating system downloads **106**
  - Checklist for effects on files and settings in the receiving terminal **107**
  - Hardware checklist **106**
  - Procedure **107**

Software checklist **106**
Performing downloads by telephone **109**
Hardware checklist **109**
Procedure **110**
Software checklist **109**
downloads
applications and related files **80**
back-to-back **79**
back-to-back application **80**
back-to-back application downloads
cable connection **101**
by telephone **79**
definition **79**
direct download utility (DDL) **80**
direct downloads
cable connections **99**
download types **82**
effect on existing files and data **98**
file authentication and back-to-back application downloads **96**
file authentication and downloading a new operating system **95**
file authentication and downloading applications to specific file groups **94**
file authentication and optimizing available memory space **97**
file authentication and timing considerations **97**
file authentication procedure for **91**
file authentication process **81**
file authentication requirements **90**
certificates and signature files **90**
file compression **98**
file groups **41**
file system organization **84**
full and partial downloads **81**
full application **82**
full operating system **83**
host PC **79**
operating system files **80**
OS files and file authentication **95**
partial application **82**
partial operating system **83**
performing a direct application download **101**
planning download tasks **84**
redirecting files during **86**
redirecting files to flash memory **86**
redirecting files to other file groups **88**
redirection of files during downloads **86**
back-to-back downloads **90**
how operating system files are redirected **89**
using DDL.EXE to automatically redirect files **89**
restrictions on redirecting files to other file groups **88**
select port **41**
select type **41**
set up the download environment for application or OS downloads by telephone **99**
set up the download environment for back-to-back application downloads **99**
set up the download environment for direct application and OS downloads **99**
setting up the download environment **99**
store the main application in File Group 1 **85**
support for multiple applications **84**
physical and logical access to file groups **85**
telephone **100**
terminal configuration settings **81**
tools **80**
types of download operations **79**
use of RAM and flash memory **85**
defragmenting the flash **86**
implications for data transfers **85**

E

electrostatic discharge **21**
error log **49, 50**

F

File authentication
Authenticating files in specific file groups **71**
Certificates
Adding new certificates **68**
Application Partition Certificate **56**
Certificate tree **65**
Customer Signer Certificate **69**
Customer Sponsor Certificate **69**
Default Signer Certificate **66, 69**
Default Sponsor Certificate **67**
Definition **55**
Development certificates **66**
Downloading Sponsor and Signer Certificates **67**
File size **73**

Hierarchical relationships **56, 65**
How certificates control file signing privileges **67**
How they are authenticated **65**
In a deployment terminal **66**
In a development terminal **66**
Main functions **65**
Platform Root Certificate **56**
Signer Certificate **57**
Sponsor Certificate **56**
What happens when you download a certificate **66**
Deciding which files to authenticate **63**
Definition of file authentication **55**
Deployment process **57, 60**
Development process **57**
Digital signature **56**
File signing
Customer Signer PIN **69**
FILESIGN.EXE **73**
Command-line mode **74**
Default inputs **69**
FileSign dialog box **74**
Graphical interface mode **74**
Required inputs **69**
Switches for command-line entries **75**
Syntax **75**
System requirements **73**
What it does **73**
For operating system files **73**
How signature files authenticate application files **64**
Required inputs to the file signing process **68**
Using the Signer Private Key **57**
For development terminals **66**
For non-executable application files **63**
Guidelines for downloading specific file types **73**
Keys
Customer Signer Private Key **69**
Default Signer Private Key **69**
How private cryptographic keys are conveyed to customers **56**
Private cryptographic key **56**
Public cryptographic key **65**
Relationship to signature files **56**
Planning for successful file authentication **62**
Pre-deployment process **57, 59**
Process flow
Confirming successful authentication **64**
Effect of failed authentication **64**
Running the *GO application following authentication **64**
Visual and audible indications during processing **64**
When the ATTR_NOT_AUTH bit is set **65**
Relationship to file groups **70**
Signature files
File size **73**
Special files used in the file authentication process **56**
VeriFone PKI
How certificates ensure logical security **65**
VeriFone Certificate Authority **55**
VeriShield security architecture **55, 63**
file authentication **90**
and downloads **91**
back-to-back downloads **96**
downloading OS files and **95**
file group password **36**
file groups **35**
keyed records **45**
password **36, 41, 47**
passwords **42**
store main application in Group 1 **85**
files
CONFIG.SYS **48**
keyed **48**
placing in terminal directories **86**
flash **41**
clear all files **42**
defragment **42**
display memory used **44**
flash memory
defragment **40**
downloads to **40**
full application download **82**
full download **41**
full OS download **106**
Function keys
ALPHA **29**
BACKSPACE **29**
CANCEL **29**
Descriptions **29**
ENTER **31**
Using terminal keys **27**

I

installation
- connecting a PIN pad **24**
- connecting a smart card reader/writer **24**
- connecting optional device(s) **23**
- connecting the terminal power pack **25**
- connecting the terminal to a telephone line **19**
- MSAM cards **21**
- MSAM holders **21**
- peripherals **24**
- setting up a direct telephone line connection **19**
- table of peripheral devices **23**
- terminal location **17**
- unpack the shipping carton **18**

integrated PIN pad **45**
- diagnostic **52**
- key loading mode **52**

K

key value **46, 48**
keyboard test **51**
keyed files **48**
keyed records **45**
Keypad
- 16-key core keypad **28**
- Troubleshooting **119**

Keys. See Function keys, Programmable function keys.

M

magnetic card reader test **51**
Maintenance
- Returning a terminal **120**

memory space
- optimization **97**

Messages
- Troubleshooting **117**

modem country code **45**
modem type **45**
MSAM cards **21**
MSAM holders **21**

N

Non-protected records **48**

O

operating system downloads **83**
optimize memory space **97**
optional devices, connecting **23**

P

paper rolls
- for thermal printer **19**

partial application downloads **82**
partial download **41**
partial OS download **106**
password **34, 36**
passwords **35**
- file group **42, 47**
- manufacturer's default **44**

peripherals
- cables **123**
- check readers **24**
- installation **24**
- PINpad **24**
- printers **24**
- smart card reader/writers **24**
- table of supported devices **23**

PIN pad **45**
PINpad
- connecting **24**

Port pinouts **137**
ports
- downloads and **41**

power pack
- AC version **123**
- connecting **25**
- DC version **123**
- ordering **123**

Printer
- Troubleshooting **118**

printer
- display information on **52**
- paper roll spindle **123**

printer paper
- ordering **123**

Programmable function keys
- Descriptions **31**

Protected records **48**

R

RAM **41**
clear **42**
display memory used **44**
Remote diagnostics
For troubleshooting **117**
reset date and time **45**
restart the terminal **40**

S

SecureKit **53**
Service **117**
Returning a terminal **120**
signature file **73**
smart card reader/writer
connecting **24**
System Mode
CONFIG.SYS **48**
system mode **33**
debugging applications in **51**
diagnostics in **51**
display memory used **44**
display panel test **51**
download port selection **41**
download type **41**
entering **38**
error log display **49, 50**
file group password **42**
file groups **35, 41**
integrated PIN pad **45**
IPP test **52**
keyboard test **51**
local and remote operations **33**
mag card reader test **51**
menu 1 **39**
menu 2 **40**
menu 3 **43**
menu 4 **49**
menu 5 **51**
menu 6 **52**
menus **36**
password **47**
procedures **37**
RAM **42**
restart the terminal **40**
terminal downloads **41**
tests **51**
System Mode operations
Protected and non-protected records **48**
system password **35**

T

telephone downloads **100**
telephone line connections **19**
direct **19**
telephone line cord, ordering **123**
Terminal
Accessories **123**
Core keypad **28**
Data entry modes **28**
Documentation **123**
Key descriptions **29, 31**
Repair **120**
Replacement **120**
Service **117**
Service and support **120**
Specifications **122**
Troubleshooting **117, 118**
Using terminal keys **27**
terminal
clock **40**
configuration information **44**
downloads **41**
file editor **48**
life of **45**
number of resets **45**
password **34, 35**
restart **40**
verify status **34**
tests
display panel **51**
integrated PIN pad **52**
keyboard **51**
magnetic card reader **51**
Thermal printer
Troubleshooting **118**
thermal printer
about thermal printer paper **19**
time **40**
timing considerations and downloads **97**

Troubleshooting **117**
- Display **118**
- Guidelines **117**
- Keypad **119**
- Printer **118**
- Serial port connection **118**
- Smart card reader **117**
- Terminal transactions **118**
- Using remote diagnostics **117**
- Using system messages **117**

U

upload **79**

V

VeriCentre 2000 **80**
VeriCentre Download Management Module **48**

VeriFone, Inc.
2455 Augustine Drive
Santa Clara CA 95054-3002
Tel: (800) VeriFone (837-4366)
www.verifone.com

Omni 37xx Series

Reference Manual

VeriFone Part Number 22412, Revision A